digital whisper
Technologic Papers

סקירה על דיני הגנת הפרטיות ויסודות בפרטיות

נכתב ע"י עו"ד יהונתן קלינגר

הקדמה

הזכות לפרטיות אינה זכות מוגדרת וברורה כמו חופש התנועה, חופש הביטוי או הזכות לקניין אשר ניתן להבין בצורה פשוטה ובמשפט אחד; מדובר בזכות שברורה לכולנו ואנו מבינים מהי, אך איננו יכולים להגדירה בצורה מושלמת. בסוף המאה ה-19 הגדירו סמואל וורן ולואיס ברנדייס את הזכות כזכות להנות מהחיים - הזכות להעזב בשקט. אבל דומה שהיום, בעת שהטכנולוגיה מתקדמת, אנחנו לא יכולים לומר בוודאות שאם נעזב בשקט פרטיותנו תסופק. הרי, אפשר לחשוב על כל מיני דרכים בהן אדם עדיין 'נעזב בשקט' אבל עדיין מרגיש שפרטיותו נפגעת: הדוגמא הטובה ביותר לכך היא של פרופיילינג, בו אנחנו נעזבים בשקט, אבל המידע שאוספים עלינו משמש כדי לא לעזוב אחרים בשקט.

בארץ, דיני הגנת הפרטיות הם פשוטים; שני חוקים מגדירים את הזכות לפרטיות בצורה כללית, וכמה חוקים בודדים עוסקים בזכות בצורה יותר ספציפית. נתחיל בחוקים הכלליים, והם חוק יסוד כבוד האדם וחירותו שסעיף 7 בחוק מגדיר ארבע זכויות שונות לפרטיות: (1) זכאות לפרטיות וצנעת חיים; (2) איסור על כניסה לרשות היחיד; (3) איסור חיפוש ברשות היחיד, בגוף או בכלים; (4) איסור על פגיעה בסוד שיחה, כתבים או רשומות של אדם. ארבע הזכויות הפשוטות האלה לא מצליחות להגדיר את הפרטיות מספיק טוב, בהתחשב בכך שלמרות חוק היסוד יש לא מעט פגיעות שמבוצעות ביום-יום, אלא דווקא בגלל שהגבולות כבר אינם אותם גבולות שהיו ב-1992, כשעבר חוק היסוד. לדוגמא, ההגדרה "רשות היחיד", שהייתה כה ברורה כאשר היה ברור שביתו של אדם הוא מבצרו, אינה רלוונטית כאשר "רשות היחיד" אינה המקום בו אדם שומר את המידע הרגיש ביותר שלו, כמו היום, בו אדם מחזיק את רוב המידע הרגיש שלו בענן ובאינטרנט.

במקביל, חוק הגנת הפרטיות, שקודם לחוק היסוד, קובע רשימה של מקרים שיחשבו כפגיעה בפרטיות: (1) בילוש או התחקות אחר אדם; (2) האזנה אסורה; (3) צילום אדם ברשות היחיד; (4) פרסום צילום אשר עלול לבזות או להשפיל אדם; (5) פרסום תמונה של נפגע בצורה מזהה; (6) העתקת מכתב ופרסומו; (7) שימוש בשמו של אדם לצרכי רווח; (8) הפרה של חובת סודיות בחוק; (9) הפרה של חובת סודיות בהסכם; (10) שימוש במידע על ענייניו הפרטיים של אדם שלא למטרה שהיא נמסרה; (11) פרסום של מידע שהושג תוך פגיעה בפרטיות; (12) פרסום של עניין הנוגע לצנעת חייו האישיים של אדם, כגון עבר מיני או מצב בריאותי.

בנוסף יש שורה של חוקים שעוסקים בפרטיות באופן פרטני, כמו חוק האזנות סתר, שאוסר על האזנה לשיחות של אדם, חוק מידע גנטי, שקובע הסדרים הקשורים למטען גנטי של אדם, חוק זכויות החולה ששומר על סודיות המידע הרפואי של אדם ועוד חוקים שונים. כלומר, הזכות לפרטיות כה קשה להגדרה שאי אפשר במשפט אחד לארגן אותה בצורה מובנת.

מנגד, יש שורה של חוקים שהינם הסדרים שמטרתם לפגוע בפרטיות בצורה שנחשבת סבירה ומידתית. כך, לדוגמא, חוק נתוני תקשורת שמיועד להסדיר את השימוש במידע שקשור למיקומו של אדם באמצעות הטלפון הסלולרי שלו (שאושר לאחרונה בבג"ץ 3809/08 האגודה לזכויות האזרח נ' משטרת ישראל) וחוק המאגר הביומטרי מסדירים בעמודים רבים וסעיפים ארוכים רק את הפגיעה בפרטיות שנובעת מההסדרים שמעבירים לרשויות השלטון מידע על בני אדם.

דיני מאגרי מידע בכלל

דיני מאגרי המידע הכלליים (להבדיל ממאגרים ספציפיים כמו המאגר הביומטרי) מוסדרים בפרק ב' לחוק הגנת הפרטיות. הכלל הוא, כי למעט מספר חריגים מצומצם, כל "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב" הם מאגר מידע, כאשר מידע מוגדר בחוק כ-"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". כלומר, קודם כל, מאגרי מידע, ככלל, חייבים להיות ממוחשבים. מאגר שאינו ממוחשב, כמו חוברת המכילה מידע, יכולה להיות כפופה לחוקים אחרים, אך לא לחוק הגנת הפרטיות.

החלק השני הוא החריגים: ככלל, מאגר מידע חייב ברישום במשרד המשפטים. אלא, שיש כמה סוגים של מאגרים שאינם חייבים ברישום, וישנם כמה סוגי מאגרים שאינם מוגדרים כמאגרים כלל.

מה אינו מאגר?

החוק מכיל שני חריגים להגדרת המאגר, הראשון הוא "אוסף לשימוש אישי שאינו למטרות עסק" והשני הוא "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". ההגדרה הראשונה ברורה: ספר הטלפונים שלי בבית, או ספר המשפחה שאחזיק אינו מאגר מידע; הבעיה מתחילה בחריג השני: כיצד אפשר לדעת מהו אפיון שיש בו פגיעה בפרטיות? האם, לדוגמא, חנווני שמנהל תרשומת במכולת של חובותיהם של לקוחות שרושמים יוצר אפיון שיש בו פגיעה בפרטיות?

התשובה היא לכאורה כן. בהתחשב בכך שמצבו הכלכלי של אדם מוגדר כחלק מהתחומים אשר החוק מגן עליהם, הרי שרישום במכולת, לדוגמא, יהווה גם מאגר מידע בחוק.

אלו מאגרים חייבים ברישום?

חשוב לזכור כי גם אם מאגר מסוים אינו חייב ברישום, הדבר לא אומר שאין לעמוד על דרישות אבטחת המידע בחוק. סעיף 8(ב) לחוק קובע חמישה תנאים לחובת הרישום, אשר הם חליפיים. כלומר, די שאחד התנאים יתקיים כדי להקים את חובת הרישום: "מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000; או יש במאגר מידע רגיש [נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו או כל מידע אחר ששר המשפטים קבע ככזה], המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה; המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23; המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג".

יש לקחת בחשבון שכמעט כל מידע הוא מידע רגיש, ולכן חייב ברישום. לכן, קשה לחשוב על מאגר מידע שלא יהיה חייב ברישום. מעבר לכך, כל מאגר שמכיל מידע על אנשים ולא נמסר על ידיהם, כמו מידע שנלקח מספר הטלפונים או נאסף מרשתות חברתיות, הוא גם מאגר החייב ברישום.

חובות בעל מאגר

ככלל, כל מאגר מידע, בין אם רשום ובין אם לא, חייב לעמוד על מספר זכויות של בעלי המידע (האנשים שהמידע ששמור עליהם מאוחסן). הראשון הוא החובה בסעיף 11 לחוק. חובה זו קובעת כי לפני שאוספים את המידע חובה לפנות לבעל המידע ולומר לו האם יש עליו חובה חוקית למסור את המידע, מה המטרה לשמה נמסר המידע ולמי יימסר המידע ומהי מטרת המסירה. מנגד, סעיף 13 לחוק קובע כי כל בעל מידע זכאי לעיין במאגר. שתי זכויות אלה נדונו לאחרונה בהנחיה ארוכה של הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים אשר דנה במכוני מיון. באותו הנושא, הרשות קבעה כי מכון מיון לעבודה לא יכול למנוע ממועמדים לעיין במידע שנשמר עליו, וכן לא יכול להתנות את קיומן של הבחינות בוויתור גורף על הזכות לפרטיות. כעקרון, כל מאגר מידע חייב לעמוד בשתי חובות אלה, לעיין ולדעת מהי מטרת המידע. ללא עמידה בהן, המאגר יהא מפר חוק.

עקרון צמידות המטרה

עקרון צמידות המטרה בפרטיות קובע כי ניתן לעשות שימוש במידע רק למטרה לה הוא נמסר. כלומר, אם אדם מוסר מידע למטרה א', אסור להשתמש בו לכל מטרה אחרת. בית הדין הארצי לעבודה דן ארוכות בכך בעע 90/08 טלי איסקוב ענבר נ' הממונה על עבודת נשים, והסביר כי המידע יכול לשמש רק למטרה

שלשמה נאסף: "שימוש במידע פרטי, חייב בעקרון להיעשות אך ורק לתכלית לשמה נאסף מלכתחילה. ככל שמידע פרטי אמור להיות מעובד למטרות אחרות מאלה עבורן לוקט מלכתחילה, על המעסיק לוודא שלא נעשה במידע שימוש למטרות זרות למטרות עבורן נאסף, ועליו לנקוט באמצעים הנדרשים כדי למנוע מתן משמעות שגויה כתוצאה משינוי ההקשר".

חובות אבטחת מידע: הצפנה, גיבוב ושמירת מידע פרטי

סעיף 17 לחוק קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע"; אלא, שההגדרה של מהי אבטחת מידע לא מופיעה בצורה מפורשת. בשנת 2010 פרסמה הרשות למשפט, טכנולוגיה ומידע נייר עמדה וטיוטא של תקנות אבטחת מידע שאמורות להגדיר את אבטחת המידע במאגרי מידע; אלא, שטיוטא זו טרם הפכה לרשמית. אולם, ניתן לראות את טיוטאת התקנות כיום להמלצה על מהי אבטחת מידע סבירה לפי סעיף 17 לחוק (כאן ניתן לקרוא במלואן על התקנות); לפני מספר שבועות פרסמה הרשות טיוטא חדשה להנחיות, אך גם היא טרם הפכה לסופית.

על פי ההצעה, בעל מאגר ינסח מסמך אבטחת מידע שכולל את סוגי המידע והערכת הרגישות שלהם, המטרות המותרות של השימוש, מידע על העברת מידע מחוץ לגבולות המדינה, מידע על ביצוע פעולות באמצעות מחזיק (מי שאינו בעל המאגר) והסיכונים המרכזיים בפגיעה בשלמות המידע, חשיפתו או שימוש בו שלא כדין, וכיצד עליו להתמודד עמם (תקנה 2). תקנה 2 גם מממשת את עקרון צמידות המטרה, כאשר היא קובעת כי אין לשמור מידע שאינו נחוץ וכי "בעל מאגר יתכנן, ככל הניתן מראש, את פעילות המאגר ואת מערכותיו באופן שיפחית את סיכוני אבטחת המידע למידע שבמאגר" (תקנה 2(ד)).

כלומר, עיצוב המאגר צריך להיות מראש כזה שמוכן לכשל; בין היתר, ניתן להסיק כי גיבוב של סיסמאות, מתוך הבנה כי דליפתן של סיסמאות בטקסט מלא עשויות לגרום לנזק בלתי הפיך, היא חובה מתוך מזעור הסיכונים, וכך גם שימוש במזהה חד-ערכי שאינו תעודת הזהות של אדם. הכלל הוא פשוט: **אין לשמור מידע שאין צורך בו, ומידע שמשמש רק לזיהוי צריך להיות מגובב (Hashed)**. מידע אחר, עדיף שיהיה מוצפן בצורה מאובטחת.

תקנה 3 קובעת כי על כל בעל מאגר מידע למנות "ממונה על אבטחת מידע" שצריך להיות עצמאי ותלוי רק בבעל המאגר. הממונה אמור להיות גם מי שמקבל תלונות אבל גם מי שמבצע את הבדיקות, ולכן כדי להימנע מניגוד עניינים, ראוי שהממונה לא יהיה מפתח האתר, אלא אדם עצמאי.

הממונה צריך לכתוב נהלי אבטחה (תקנה 4), אשר כוללים את רמת אבטחת המאגר, תיאור של רכיבי המערכת וקביעת הרשאות הגישה (לדוגמא, למנוע מכל אדם שעובד בחנות לראות את היסטורית הרכישות). במאגרים שחלה עליהם רמת אבטחה בינונית ומעלה (מאגרים שמשמשים לדיוור ישיר (רמה

בינונית) או שמוגדרים ברמת אבטחה גבוהה (מאגרים גנטיים, מאגרים שמכילים מידע כלכלי, מאגרים שמכילים מידע על דעות פוליטיות, נטיות מיניות או מעשים מיניים, עבר פלילי, נתוני תקשורת (שיחות או ביקור באתרי אינטרנט), מידע ביומטרי)) יש עוד לדאוג שההנחיות יכללו הוראות על רמת האבטחה הפיסית (כלומר הגישה הפיסית לשרת), אבטחת התקשורת והאחסון, גיבויים ושחזורים ובדיקות תקופתיות.

כלומר, נהלי האבטחה לא רק שצריכים להיות מקיפים, אלא במאגרים רגישים יותר (ברמה הבינונית והגבוהה) צריכים לטפל גם באבטחה הפיסית של השרת (לא כל שרת באחסון משותף בסדר) ולבדוק שאין זליגת מידע בין האחסון הזה למאגרים אחרים.

תקנה 5 קובעת כי **יש לערוך סקר סיכונים במאגרים ברמה בינונית ומעלה**; כלומר, על בעל המאגר לבדוק את מערכות החומרה ורכיבי התקשורת, לבדוק את ההתקנים הניידים בהם נעשה שימוש ואת מערכות התוכנה שמנהלות את המאגר (נניח, תוכנת הניהול). אבל הוא גם חייב לבחון את התוכנות המשמשות לתקשורת מחוץ למאגר ואת הרכיבים האחרים הדרושים להפעלת המאגר. במאגרים שאינם ברמה בינונית, יש רק לערוך פירוט של הרכיבים, ואין ממש חובה לבחון אותם.

תקנה 6 היא בעצם לב הפרשנות של חובת אבטחת המידע. כלשונה "אחראי המערכות יבטיח כי המערכות המפורטות בתקנה 5(א) יישמרו במקום מוגן, המונע חדירה אליו וכניסה בלי הרשאה והתואם את אופי פעילות המאגר ורגישות המידע בו"; שימו לב, **למרות שיש חובה להגן על המאגר מגישה לא מורשית, אין חובה להצפין מידע ובמיוחד אין חובה להצפין מידע בצורה חד-כיוונית** (כלומר, להצפין מידע כמו סיסמאות, כך שאם המאגר ידלוף אלה לא יוכלו לשמש אנשים אחרים אינה חלק מהחובות כאן); במאגרים ברמה בינונית ומעלה יש גם צורך לתעד את הגישה למאגר. לדעתי האישית, וכדי להקטין את הנזקים האפשריים, עדיף להצפין מידע קודם כל ואם אין צורך במידע אלא רק לאימות שלו (נניח, במספרי תעודת זהות, כתובות דואר אלקטרוני שמשמשות לגישה לאתר או סיסמאות) יש להשתמש בהצפנה חד-כיוונית.

תקנה 7 קובעת כי **העובדים יודרכו בנוגע למידע הרגיש ונהלי אבטחת המידע**, יחתמו על הוראות סודיות ויעברו הדרכות תקופתיות במאגרים ברמה בינונית ומעלה. תקנה 8 ממשיכה כיוון זה וקובעת כי הגישה תעשה רק על ידי עובדים שמורשים לכך (כלומר, עדיף סיסמא לכל עובד ולא סיסמא מאסטר או גישה פתוחה למאגר); **במאגרים ברמה בינונית ומעלה יש לדאוג שלאף עובד לא תהיה גישה למאגר במלואו אלא אם הדבר חיוני, וכי ביצוע פעולות חיוניות יהיה בשליטה של יותר מעובד אחד**.

תקנה 9 ממשיכה את חובות התיעוד והניהול וקובעת כי הפעילות תבוצע רק על ידי עובדים מורשים וכי במאגרים ברמה בינונית או גבוהה יקבעו גם נהלים לגבי אורך הסיסמאות, החלפתן וכדומה. כמו כן, יש לדאוג כי עובדים שסיימו את עבודתם לא יוכלו להמשיך לגשת למאגר הרגיש.

תקנה 10 קובעת כי במאגרים ברמה בינונית ומעלה יש לערוך תיעוד של הגישה למאגר ושל ניסיונות גישה שנכשלו, לשמור את המידע על הגישה לפחות לשנתיים וליידע את העובדים על העניין. תיעוד מסוג זה יכול לסייע בגילוי של שימוש לרעה במאגרי מידע בשירות המדינה (כמו בעשם 3275/07 שמואל ציילר נ' נציבות שירות המדינה בו עובד במחלקת מיסוי מקרקעין הורשע בשליפת מידע שלא כדין) שכן מערכות ניהול ותיעוד גישה קודם כל ירתיעו את המשתמשים משימוש לרעה אבל גם ישמשו כדרך לגלות את דליפת המידע מאוחר יותר.

תקנה 11 מחייבת את אחראי האבטחה לנהל תיעוד של אירועי אבטחה ובמאגרים ברמה בינונית או גבוהה אף לקבוע נהלים לטיפול באירועי אבטחה. העדכון המשמעותי כאן הוא החובה לדווח לרשם מאגרי המידע על תקלות אבטחה במקרים בהם נעשה שימוש במידע שלא בהרשאה (במאגרים ברמת אבטחה גבוהה) או בחלק מהותי מהמידע (במאגרים עם רמת אבטחה בינונית). העדכון המשמעותי כאן הוא שהרשם יכול גם לחייב את בעל המאגר ליידע את בעלי המידע.

תקנה 12 קובעת, בקצרה, כי העברה של מידע מחוץ למאגר על התקנים ניידים תעשה רק באופן שמונע שימוש לרעה בהם (כאן דווקא הצפנה נחשבת אמצעי סביר). תקנה זו נובעת, בין היתר, מכך שחדשות לבקרים שומעים אנו על כך שמאגרים שמכילים מידע רפואי נמצאים בזכרונות ניידים שנשכחים במקומות מסוימים, במאגרים ברמה גבוהה או בינונית יש גם לתעד את ההתקנים שנעשה בהם שימוש ולראות היכן נמצא כל אחד מהם, כמו גם להוציא אותם רק באישור של אחראי האבטחה.

תקנה 13 **דורשת להפריד, באופן סביר, בין מערכות המידע הרגילות לבין מערכות מחשוב אחרות וכי מאגר המידע לא יחובר לרשת בלי מערכת המונעת גישה בלתי מורשית**.

תקנה 14 דנה באבטחת התקשורת, וקובעת כי המאגר "לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה מתאימים המגנים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב" גם כאן, לא ברור מהם האמצעים המתאימים? האם די בשם משתמש וסיסמא, או שצריך two-factor authentication? חבל שהרשות לא הנחתה.

תקנה 15 דנה במיקור החוץ; לכך, כאמור, כבר פרסמה הרשות הנחיות. כשאנחנו מדברים על עולם של מערכות אחסון בענן, שירותי צד ג' שנותנים את ניהול מאגר המידע ועוד, ההנחיות יכולות להיות חשובות יותר ופי כמה. טיוטת התקנות מדברת על בדיקת נחיצות ההתקשרות במיקור חוץ, כלומר **ההנחה היא שאם ניתן לבצע את ניהול המאגר ברמה הפנימית, עדיף לעשות כן על להוציא את ניהול המאגר לגורם חיצוני**. לי אישית יש הסתייגויות מהנושא, כי כאשר מדובר בניהול של מאגר מידע רגיש יחסית, עדיף שהוא ינוהל על ידי חברה שמודעת לסיכונים ויודעת לנהל מאגרים נוספים, על חנות קטנה שאין לה את הידע. מנגד, מרגע שיותר מדי מידע נצבר במאגר מסוים, הוא הופך להיות יעד לתקיפה (כך היה

במתקפת ההאקרים האחרונה, כאשר פרצו לאתר השכן שהתארח ודרכו גנבו, כנראה, את נתוני האשראי של כולם).

מה שהוסר בין הטיוטות, וזה מעניין, הוא מה שהיה תקנה 16, שקבעה כי **מידע שאינו נחוץ ימחק**. לדוגמא, אין צורך לשמור את פרטי כרטיס האשראי לאחר ביצוע החיוב, ולכן יש למחוק אותם. כמו כן, כל מידע שנמחק ימחק בצורה שאינה מאפשרת שחזור שלו, לא סתם באמצעות שליחתו לסל המחזור אלא על ידי השמדה של המידע. סביר להניח שהכוונה היא לכך שקודם כל במקום המידע ייכתב מידע ריק וחסר משמעות, ורק לאחר מכן ימחק המידע, וכן שכל המידע הלא נחוץ יוסר מגיבויים קודמים. חשוב לזכור שאי עמידה בהוראה זו אינה שונה מפגיעה באבטחת המידע בכלל.

תקנה 16 קובעת כי **במאגרים במידת אבטחה בינונית ומעלה יערכו גם בדיקות תקופתיות לבדיקת אבטחת המידע**. גם אם אתם לא כאלה, אז כדאי להסתכל על שירותים כמו Kyplex או 6Scan שעורכים בדיקות תקופתיות לאבטחת המידע באתר שלכם, ובודקים אם תיקנתם את עדכוני האבטחה האחרונים.

תקנה 17 דנה בסוגיית הגיבויים, וקובעת **שבמאגרים ברמת אבטחה בינונית ומעלה יערכו גיבויים לפחות אחת לשבוע** (אני בכל מקרה ממליץ לגבות את המידע תמיד) וכן נהלי התאוששות לפתיחת הגיבויים. במאגרים שמוגדרים ברמת אבטחה גבוהה יש צורך שהגיבוי יהיה אף מחוץ למקום הרגיל של הארגון (כלומר, DRP: אפשרות להתאוששות במקרה אסון).

חובות אבטחת מידע במיקור חוץ

תקנה 14 דנה במיקור חוץ, והיא המעבירה אותנו לנושא הבא גם כן. הכלל הוא כי מידע המעובד צריך להישאר בתוך הארגון, וההנחה היא כי כאשר מידע יוצא מתוך מאגר המידע לגורם שלישי,אשר הוא אינו הנהנה ממנו, ישנה השלכה על כך. לצורך כך, הרשות למשפט, טכנולוגיה ומידע הוציאה הנחיה הנוגעת לעיבוד מידע אישי במיקור חוץ, כאשר מהות ההנחיה נועדה גם להסדיר את נושא האבטחה, וגם לקחת בחשבון זכויות נוספות. בין היתר, ההנחיה שואלת שאלות קשות, שיש לעמוד בהן.

האם מותר להוציא את המידע?

השאלה הראשונה בהנחיה, 3.1.1.1 היא **האם מותר כלל להוציא את השירות למיקור חוץ**. לדוגמא, כאשר מדובר על מידע רפואי, סעיף 19 לחוק זכויות החולה קובע כי "מטפל, ובמוסד רפואי - מנהל המוסד, ינקטו אמצעים הדרושים כדי להבטיח שעובדים הנתונים למרותם ישמרו על סודיות העניינים המובאים לידיעתם תוך כדי מילוי תפקידם או במהלך עבודתם"; האם יש בכך כדי לאסור על העברת המידע לגורמים שלישיים? יכול להיות שכן. יש מקרים מובהקים יותר, כגון מאגרי מידע של רשויות ממשלתיות, אשר מחזיקות מידע על פי חוק; לדוגמא, סעיף 18 לפקודת הסטטיסטיקה (הפקודה שמתוכה

פועלת הלשכה המרכזית לסטטיסטיקה) קובע כי "דו"ח אישי שניתן לעניין פקודה זו, לא יהא מי שאינו עובד רשאי לראות אותו או חלק ממנו אלא לצרכי תביעה לפי פקודה זו". כלומר, רק עובדים שעוסקים בעיבוד המידע עבור הלמ"ס רשאים לקבל גישה למידע.

הרשאות הגישה

השאלה הבאה עליה על בעל המאגר לענות היא מהו היקף הגישה לו יהיה זכאי הגורם שמעבד את המידע במיקור חוץ, כאשר ברירת המחדל היא שהמאגר ישמר אצל בעל המאגר ונותן השירות יהיה רק זכאי לגשת אליו. האפשרויות האחרות הן איסוף כל המידע על ידי נותן השירות, או החזקה של המאגר במלואו על ידי נותן השירות. חלופות אלה מסכנות את בעל המאגר, כיוון שהן גורמות לכך שהשליטה הבלעדית תצא מידיו. ההנחה היא שככל שהמידע רגיש יותר, וככל שהאחריות כבדה יותר, על בעל המאגר להחזיקו אצלו.

בחירת הקבלן והסכם ההתקשרות

הרשות למשפט וטכנולוגיה מטילות הנחיות כבדות על בחירת הקבלן, עד כדי כך שלאחרונה הרשות נקטה בפעולה אקטיבית כדי לטפל בחברה שלכאורה הפרה את הוראות ההנחיה; הכלל הוא שעל נותן השירות יש איסור על ניגוד עניינים ויש צורך שיהיה מנוסה בעיבוד מידע אישי, הסכם ההתקשרות חייב לוודא כי נותן השירותים עומד בעקרונות החוק, כלומר אינו אוסף מידע שלא ברשות ומאפשר את חובות העיון וההודעה. כמו כן, נותן השירות חייב להעמיד בטוחות למקרה בו אכן תופר פרטיות, כדי לכפר על הנזק.

מסמך אבטחה

כמו בפעילות בתוך הארגון, גם על ניהול מידע במיקור חוץ יש להכין מסמך אבטחה מחייב, וחובה שתהיה הפרדה בין המידע שנאסף על ידי נותן השירותים עבור לקוחותיו. כלומר, נותן השירותים לא יוכל לעשות שימוש במידע עבור עצמו. גם כאן, כמו בניהול מידע בתוך הארגון, יש צורך בממונה אבטחת מידע, ויש לאפשר לבעל המאגר פיקוח הולם על המערכת.

חובת שמירת המידע

הנחיה 3.1.7 קובעת כי יש לשמור את המידע אך ורק לזמן מתן השירות, ואין להותיר את המאגר לאחר סיום השירות. החריג לעניין זה הינו מקרה בו שמירת המידע דרושה על פי חוק או לצורך ביצוע התחייבויות שנותרו לאחר תום ההסכם.

חובות אבטחת מידע והגנה על פרטיות עובדים

בעבר ההנחה הייתה כי בהתחשב בכך שהעובד משתמש במחשב של המעביד, משוחח בטלפון של המעביד ונוסע ברכב של המעביד, הרי שאין לו זכות לקניין. אלא, שלאחרונה דברים השתנו (וראו גם מעקב בעבודה: טיילור, בנת' האם והזכות לפרטיות, **מיכאל בירנהק**). פסק דין שניתן בבית הדין הארצי לעבודה (עע 90/08 טלי איסקוב ענבר נ' הממונה על עבודת נשים) יחד עם הנחיה של הרשות למשפט וטכנולוגיה בנושא פרטיות עובדים, שינו את הנחת המוצא הזו.

כיום הכלל הוא כי "**מתחם הפרטיות אינו נקבע עפ"י דיני הקניין והזכות לפרטיות היא זכותו של האדם ולא זכותו של המקום**, וכלל זה חל גם כאשר תוכן הודעת הדוא"ל הוא בעניין עסקי. גם העובד במישור של יחסי עובד-מעביד זכאי למתחם פרטיות במקום העבודה כאשר הוא משתמש בדוא"ל בשרת החברה, וכל שכן בעל מניות בחברה במישור מערכת היחסים בין בעלי המניות בחברה" (ה"פ 1529/09 חן בת שבע ואח' נ' יוני בן זאב). גם במסגרת של בדיקות אבטחה, ישנו איסור על שימוש במידע פרטי על עובדים, וככל שזה יוצג בפני בית המשפט, הרי שהוא יפסל משימוש בתור ראיה (עמר"מ 13028-04-09 בנימין אליהו נ' עיריית טבריה)

עקרון ראשון שמוזכר בטיוטת ההנחיה של הרשות למשפט, טכנולוגיה ומידע הוא עקרון ההסכמה מדעת. ההנחה היא שמערכת האיזונים במקום העבודה היא כזו שלא מאפשרת לקבל הסכמה אמתית מעובדים; "מעמדה של הזכות לפרטיות כזכות יסוד וכן אופייה המיוחד, מחייבים, כי פגיעה בפרטיות העובד תיעשה רק אם קיימת למעביד סמכות מפורשת לנהוג כך, ואין די בהסתמכות על כוחו של המעביד לנהל את המפעל על פי מיטב שיקול דעתו" (ו' וירט-ליבנה "הזכות לפרטיות אל מול האחריות הניהולית במיון מועמדים לעבודה - ההיבט המשפטי" ספר שמאגר מאמרים חלק ג' (2003) 775, 805). כלומר, ההנחה היא שעובד, אשר נאמר לו "הסכם לכך שנקרא את הדואר האלקטרוני שלך או שלא תקבל את הזכות לעבוד כאן" יוותר על הזכות לפרטיות שלו כיוון שאחרת אין לו דרך אמתית לעבודה. לכן, קביעת רמו"ט היא כי "**תוקפה של הסכמה של עובד לאיסוף או לשימוש במידע לפי החוק בידי מעביד, אינה בעלת משקל רב, אלא אם ברור מהנסיבות כי ניתנה באופן חופשי לגמרי**". כלומר, המעסיק הוא זה שצריך להראות כי העובד הסכים לפגיעה בפרטיותו.

תכלית ראויה

הדרישה השנייה בכניסה לפרטיות העובד היא עמידה בתכלית ראויה; רמו"ט קובעים כי " לכן עבור כל פריט מידע שנאסף, על המעסיק להיות מסוגל לספק הסבר משכנע לתכלית איסוף המידע". כך, לדוגמא, שעוני נוכחות ביומטריים, אשר אוספים את טביעות האצבע של העובדים, לא בהכרח יעברו בקריטריון זה, כיוון שלא בטוח שיש הסבר משכנע לכך שיש נחיצות לשימוש דווקא בטביעת האצבע (ראו, לעניין זה).

מידתיות

ההנחה היא כי אם ישנן מספר חלופות טכנולוגיות, על המעביד לבחון את האפשרות שתפגע בפרטיות העובדים בצורה הפחותה ביותר. לדוגמא, בעניין דמ"ר 39840-04-10 לודמילה לשצינר נ' פאר מרכז החלמה רפואי פסק בית המשפט כי התקנת מצלמות במקום העבודה אשר מצלמות עובדים היא פגיעה בלתי מידתית בפרטיותם; "הפעלת המצלמות בזמן שהתובעת נמצאת ו/או עובדת בחדר שהוקצה לה, מהווה פגיעה לא מידתית ולא סבירה בפרטיותה של התובעת". כך תהא התוצאה גם במקרים דומים, וראוי לבחון כל פגיעה ופגיעה.

שקיפות

הכלל הוא כי גם על מעביד לפעול לפי סעיף 11 לחוק, וליידע את העובד האם הוא חייב לתת את המידע או לאו, מה יהיה השימוש במידע והיכן המידע יאוחסן ויאובטח.

הגבלת מטרה

ישנו איסור על מעביד לעשות שימוש במידע שלא למטרה שהעובד מסר. לדברי רמו"ט, "על המעביד לוודא כי כל השימושים הנעשים במידע ייעשו רק למטרה שלשמם נמסרו. החובה לקיים את השימוש והמטרה הינה על המעביד בכל מקרה קונקרטי".

סודיות ואבטחת מידע

לדברי הרשות למשפט, טכנולוגיה ומידע, אין הבדל בין שמירת מידע כללי לבין שמירת מידע על העובדים מבחינת דיני מאגרי המידע. כלומר, שעון הנוכחות של העובדים והגישה לתיקי כוח האדם צריכים להיות מוגנים בדיוק באותה סודיות שמוגן מאגר המידע הרלוונטי על לקוחות העסק.

מיקור חוץ

העקרונות שהוצאו בהנחיה הנוגעת למיקור חוץ חייבים לחול גם על מיקור חוץ הנוגע לעובדים. לדברי הרשות למשפט, טכנולוגיה ומידע, "על ארגון המעבד מידע באמצעות מחזיק חלה החובה להסדיר בחוזה מחייב, כחלק מהגדרת השירות, גם את ההוראות הרלבנטיות החלות בתחום הגנת הפרטיות, ולוודא גם לאחר החתימה על החוזה, כי המידע האישי מנוהל כראוי. על ארגון המעביר מידע למיקור חוץ חובה נמשכת לוודא כי המידע מטופל כראוי".

עיון ותיקון

החובה לאפשר לבעל המידע לעיין חלה גם על מידע הנוגע לעובדים. כך, לדוגמא, הסוגיה של עיון בחוות דעת של מנהלים, ככל שאלה מאוחסנות במאגר המידע, צריכה לחול גם כאן.

מסקנות קונקרטיות

ההנחה היא שבעקבות הלכת טלי איסקוב למעסיקים אסור להכניס לתחום הפרטי של עובדיהם. ככלל, מעסיק לא יכול לקרוא את הדואר האלקטרוני של העובד גם אם זה הסכים לכך בחוזה העבודה, אלא ההסכמה צריכה להיות ספציפית במיוחד. לדברי בית הדין: "הסכמת העובד שני פנים מצטברים לה: נדרשת הסכמת העובד מראש, מרצון ומדעת למדיניות הכללית הנוהגת אצל המעביד בכל הנוגע לפעולות מעקב וחדירה לתיבות דואר שהועמדו לשימושו האישי. בנוסף ובמצטבר נדרשת הסכמת העובד הספציפית בגין כל פעולת מעקב וחדירה בנפרד לתכתובת אישית, ככל שבכוונת המעסיק לקיימן. וזאת, בשים לב לסוגים השונים של תיבות הדואר והשימוש האישי האסור והמותר במסגרתן".

סיכום

דיני הגנת הפרטיות הפכו להיות מהותיים יותר כאשר בחלק מהמקרים תכליתם היא להגשים את חובות אבטחת המידע ובמקרים אחרים הן מצרות את ידיהם של מי שאמון על אבטחת מידע שכן הוא אינו יכול לגשת למידע כדי לבדוק האם הופרה האבטחה. היום, יותר מתמיד, יש על איש אבטחת המידע לעבוד בצמוד לעורך דין, על מנת שידע מה אסור, מה מותר ומה רצוי.