משרד המשפטים

הצוות לבחינת החקיקה בתחום מאגרי המידע

דין וחשבון

ירושלים, שבט, התשס"ז
ינואר, 2007

ירושלים, ב׳ בשבט, תשס״ז
21 בינואר, 2007

לכבוד
<u>שרת המשפטים</u>

שלום רב,

הנדון: <u>דו״ח צוות לבחינת פרק ב׳ בחוק הגנת הפרטיות</u>

אנו מתכבדים בזאת להגיש לך את דו״ח הצוות לבחינת פרק ב׳ בחוק הגנת הפרטיות, התשמ״א-1981, בראשות המשנה ליועץ המשפטי לממשלה (חקיקה).

הצוות בחן את ההסדר החוקי הראוי בנוגע להסדרת תחום מאגרי המידע. עבודת הצוות נמשכה כשנתיים בהן קיים הצוות מספר ישיבות ובחן את ההסדר הקיים למול הסדרים משפטיים אחרים.

עם סיום עבודת הצוות, רוכזו המלצותיו בדו״ח. דו״ח זה כולל גם המלצות לתיקון החקיקה הקיימת בנושא.

בברכה,

חברי הצוות

העתק:
היועץ המשפטי לממשלה
מנכ״ל משרד המשפטים

יהושע שופמן, עו"ד
המשנה ליועץ המשפטי לממשלה (חקיקה)
יו"ר הצוות

חיים קלוגמן, עו"ד
יו"ר המועצה להגנת הפרטיות

יוספה טפיירו, עו"ד
רשמת מאגרי המידע, משרד המשפטים

דלית דרור, עו"ד
ראש תחום משפט ציבורי,
מחלקת ייעוץ וחקיקה, משרד המשפטים

חיים רביה, עו"ד
רביה ושות', עורכי דין
וחבר המועצה להגנת הפרטיות

מר נחמן ליס,
האחראי על הפיקוח, יחידת רשמת מאגרי
המידע, משרד המשפטים

מר בובי פיינדריך,
ראש אגף אבטחת המידע,
המוסד לביטוח לאומי

מיכאל בירנהק, ד"ר
הפקולטה למשפטים, אוניברסיטת חיפה
וחבר המועצה להגנת הפרטיות

אבנר פינצ'וק, עו"ד
האגודה לזכויות האזרח
וחבר המועצה להגנת הפרטיות

יובל אלוביץ', ד"ר
המחלקה להנדסת מערכות מידע,
אוניברסיטת בן-גוריון

ברכה שפירא, ד"ר
המחלקה להנדסת מערכות מידע,
אוניברסיטת בן-גוריון

עומר טנא, ד"ר
המסלול האקדמי המכללה למינהל

עמית אשכנזי, עו"ד
עוזר ראשי, מחלקת ייעוץ וחקיקה,
משרד המשפטים

רבקי דב"ש, עו"ד
מחלקת ייעוץ וחקיקה, משרד המשפטים
רכזת הצוות

תוכן העניינים

1 - מבוא......5

1.1 - חברי הצוות......6
1.2 – רקע היסטורי......7
1.3 – הסדרים בשיטות משפט אחרות......9
1.4 - מבנה הדו"ח......12

2 - היקף התחולה של פרק ב'......13

2.1 - תאגיד כנפגע פוטנציאלי......13
2.2 – החלת החוק על מאגרי מידע שאינם ממוחשבים......16

3 - הגדרות......19

3.1 – הגדרת "מידע"......19
3.2 – הגדרת "מידע רגיש"......21

4 - חובת רישום מאגרי מידע......24

4.1 – חובת הרישום......24

5 - סמכויות רשם מאגרי מידע......28

5.1 – סמכויות הרשם......28

6 - המועצה להגנת הפרטיות......34

6.1 – עיגון מעמד המועצה בחקיקה......34

7 - חובות הנלוות לניהול מאגר מידע......35

7.1 - חובות מקדמיות על בעל המאגר ומחזיקו......35
7.2 - מתן הודעה על איסוף מידע......38
7.3 – העברת מידע ממאגר המידע......41
7.4 - אבטחת מידע......42
7.5 – אבטחת מידע במאגרי מידע ממשלתיים......46
7.6 – סודיות......48

8 – זכות העיון והתיקון......50

8.1 –זכות העיון......50
8.2 – עלות זכות העיון......53
8.3 – השפה בה יימסר המידע......54
8.4 – זכות התיקון......55
8.5 – מאגרים שאינם פעילים......57

9 – פטור למאגרים מיוחדים מזכות העיון ומחובת ההודעה......58

9.1 – פטור ממתן זכות עיון......58
9.2 - פטור ממתן הודעה......61

10 - דיוור ישיר......62

10.1 – דיוור ישיר......62
10.2 – אבחנה בין שרותי דיוור ישיר לדיוור ישיר......65

11 - העברת מידע לחו"ל......67

11.1 – העברת מידע לחו"ל......67

12 – סיכום......69

12.1 - תמצית החלטות הצוות......69
12.2 – סוף דבר......71

13 – נספח......72

טכנולוגיה ופרטיות – משפט משווה*......72

1 - מבוא

במהלך הכנת תזכיר חוק הגנת הפרטיות (תיקון - פרטיות של נפטר, הסכמה מדעת ופיצוי ללא הוכחת נזק), התשס"ד – 2004[1] (להלן – **תזכיר החוק**) התגבשה במחלקת ייעוץ וחקיקה ההכרה כי בתחום מאגרי המידע יש צורך בבחינה מחדש של ההסדר החוקי כמכלול, ואין להסתפק בתיקוני חקיקה נקודתיים. הצורך בבחינת החקיקה נבע ממספר טעמים אשר הראשון בהם הוא חלוף הזמן מאז נחקק פרק ב' לחוק הגנת הפרטיות, התשמ"א-1981[2] (להלן – **חוק הגנת הפרטיות**), כאשר בין לבין נחקק חוק יסוד: כבוד האדם וחירותו אשר עיגן את הזכות לפרטיות כזכות חוקתית (סעיף 7 לחוק היסוד). כמו כן, החידושים הטכנולוגים הובילו לכך שהשימוש במאגרי מידע, כהגדרתם בחוק הגנת הפרטיות, נעשה באופן תדיר המקיף את כל תחומי החיים המודרניים. החידושים הטכנולוגיים הובילו לשכלולן של המערכות הקיימות ויצירת אפשרויות טכנולוגיות חדשות שלא היו קיימות ערב חקיקת חוק הגנת הפרטיות[3].
בנוסף, נעשה ניסיון לבחון את ההסדר הישראלי מול הסדרים שונים בעולם, ובראשם ההסדר באיחוד האירופי. לעניין זה נציין כי הצורך לבחון את החקיקה בא למנוע מצב בו זרימת מידע בין ישראל למדינות אחרות תפגע בשל סטנדרטים שונים בהגנה על הפרטיות ובאבטחת מידע, דבר העלול להוביל לפגיעה בשיתוף פעולה בתחומים שונים.
נציין כי מזה זמן מה המועצה להגנת הפרטיות (להלן – **המועצה**) קוראת לשינוי המצב החוקי הקיים, וזאת בעיקר סביב עמדתם של חלק מחברי המועצה בדבר כישלון הסדר רישום מאגרי המידע.

לאור כל זאת עלה הצורך להרכיב צוות של מומחים, משפטנים ושאינם משפטנים, הן מקרב המערכת הממשלתית והן מחוצה לה, כדי לתת את הדעת לצורך בשינוי החקיקה על מנת להתאים את החוק למציאות הקיימת, וליישם לקחים שהופקו במשך השנים תוך כדי יישום הוראותיו של החוק.

הצוות התבקש **"לבחון ולהמליץ למשרד המשפטים על הסדרת החקיקה בנושא מאגרי מידע (Data Protection) - בחינת ההסדר הרצוי, הגדרת תחולת ההסדר ואמצעי האכיפה."** בנוסף הוחלט על בחינה מחודשת של פרק ד' של חוק הגנת הפרטיות (להלן – **פרק ד'**) על ידי צוות נפרד. אי לכך דו"ח זה לא יעסוק בסוגיה של העברת מידע בין גופים ציבוריים.

---

[1] פורסם, תוך כדי השמטת הסעיפים הנודעים לפרק ב לחוק, כהצעת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ו-2005 בה"ח התשס"ו, עמ' 230.
[2] פרק ב' נתקבל בכנסת כחלק מחוק הגנת הפרטיות בשנת 1981 ופורסם בס"ח התשמ"א, עמ' 128.
[3] כגון: האינטרנט, data mining, רוגלות נגישות וכד'

1.1 - חברי הצוות

הצוות מנה את החברים הבאים:
מר יהושע שופמן, המשנה ליועץ המשפטי לממשלה (חקיקה) – יו"ר הצוות
מר חיים קלוגמן, יו"ר המועצה להגנת הפרטיות
גב' יוספה טפיירו, רשמת מאגרי המידע (כתוארה דאז), משרד המשפטים
גב' דלית דרור, ראש תחום משפט ציבורי, משרד המשפטים
מר חיים רביה, רביה ושות', עורכי דין, חבר המועצה להגנת הפרטיות
מר נחמן ליס, הממונה על הפיקוח, יחידת רשם מאגרי המידע, משרד המשפטים
מר בובי פיינדריך, ראש אגף אבטחת המידע, המוסד לביטוח לאומי
ד"ר מיכאל בירנהק, מרצה בכיר בפקולטה למשפטים באוניברסיטת חיפה וחבר המועצה להגנת הפרטיות
מר אבנר פינצ'וק, עו"ד באגודה לזכויות האזרח בישראל וחבר המועצה להגנת הפרטיות
ד"ר יובל אלוביץ', מרצה במחלקה להנדסת מערכות מידע, אוניברסיטת בן-גוריון
ד"ר ברכה שפירא, מרצה במחלקה להנדסת מערכות מידע, אוניברסיטת בן-גוריון
ד"ר עומר טנא, בית הספר למשפטים המסלול האקדמי המכללה למינהל
מר עמית אשכנזי, מחלקת ייעוץ וחקיקה, משרד המשפטים
גב' רבקי דב"ש, מחלקת ייעוץ וחקיקה, משרד המשפטים – רכזת הצוות

כמו כן, השתתפו בחלק מישיבות הצוות מוזמנים נוספים שלא נמנו עם חבריו.

לאחר שהצוות סיים את דיוניו, ובטרם פורסם הדו"ח, הוקמה במשרד המשפטים הרשות למשפט ולטכנולוגיית מידע. מר יורם הכהן נבחר לעמוד בראש הרשות ומונה כרשם מאגרי המידע. הרשות והעומד בראשה לא היו שותפים, על כן, לעבודת הצוות, ויישום ההמלצות ייעשה, כמובן, בתיאום עם הרשות ותוך התחשבות בתפקידים אותם היא תמלא.

חברי הצוות שאינם עובדי ציבור השתתפו בדיונים בהתנדבות. תודתו של משרד המשפטים נתונה לחברים, שתרמו מזמנם ומהידע הרב שלהם.

תודה מיוחדת נתונה לגב' רבקי דב"ש ממחלקת הייעוץ והחקיקה במשרד המשפטים, שריכזה את העבודה המשפטית ואף המינהלית של ישיבות הצוות, הכינה חומר רקע לישיבות וניסחה את טיוטת דו"ח הצוות, עליה העירו והוסיפו יתר החברים.

<u>1.1.1 - אופן עבודת הצוות</u>

עבודת הצוות ארכה קרוב לשנתיים וכללה התכנסות אחת לחודש. במהלך הדיונים נבחן המצב הקיים בישראל מול הסדרים בחו״ל, בעיקר מול ההסדר באיחוד האירופאי ובקנדה.

להלן, בתמצית, הנושאים שנדונו בצוות:

- היקף ההגנה בפרק ב׳
- הגדרת ״מידע״, ״מידע רגיש״ ו״מאגר מידע״
- חובות הנלוות לאיסוף המידע לצורך שמירתו במאגר
- זכויות בני אדם עליהם המידע נאסף
- מאגרים עליהם לא יחול הסדר עיון ותיקון
- דיוור ישיר
- חובת רישום מאגרי מידע
- סמכויות רשם מאגרי מידע
- העברת מידע לחו״ל

<u>1.2 – רקע היסטורי</u>

<u>1.2.1 – הרקע לחקיקת פרק ב׳</u>

עבודת ההכנה לקראת עיגון ההגנה המשפטית של הזכות לפרטיות במשפט הישראלי החלה במינוי ״ועדה להגנה בפני פגיעה בצינעת הפרט״, בראשות השופט יצחק כהן. הוועדה מונתה ב-20/8/74 על ידי שר המשפטים דאז, מר חיים צדוק, לבדוק **״את הדרכים להגנה על האזרח בפני פגיעה בצינעת הפרט״** ולהביא בפניו את המלצותיה לחקיקה. דו״ח הוועדה הוגש לשר באוקטובר 1976 והומלץ בו לעגן את הזכות לפרטיות בחקיקה, על פי הצעת חוק אשר נוסחה על ידי הוועדה. בהתייחס לנושא של פגיעה בפרטיות על יד מאגרי מידע ממוחשבים, קבעה הוועדה כי הנושא דורש מומחיות מיוחדת בנוסף לעבודת מחקר, ועל כן החליטה שלא לכלול הוראות מיוחדות בעניין המחשבים בהצעת החוק שגובשה על ידה. עם זאת ועדת כהן המליצה על הקמת **״ועדת מומחים מצומצמת, אשר תחקור בענין סכנת הפגיעה בפרטיות כתוצאה מפעולות כאלה ותמליץ על הדרכים למניעת סכנה כזו.״**

בתאריך 20/3/78 מינה שר המשפטים דאז, שמואל תמיר, את ״הוועדה למניעת פגיעה באזרח באמצעות מידע המרוכז במחשבים״, בראשותו של ח״כ דוד גלס, שתפקידיה היו –

א. לבחון מניעה של פגיעה באזרח באמצעות מידע המרוכז במחשבים;

ב. להמליץ על חקיקה המסדירה את חובותיו של מחזיק ומשתמש במידע ועל זכויותיו של מושא המידע.

הוועדה הגישה את המלצותיה לשר המשפטים בינואר 1981. באותה עת, ועדת חוקה חוק ומשפט דנה בהצעת החוק הממשלתית אשר התבססה על המלצות ועדת כהן, והחליטה לאמץ את המלצות ועדת גלס כך שהן שולבו כ״פרק ב׳״ בנוסח חוק הגנת הפרטיות כפי שנתקבל בכנסת ביום י״ט באדר א׳ התשמ״א (23 בפברואר 1981).

החוק תוקן מאז מספר פעמים, כאשר התיקונים העיקריים הנוגעים לענייננו היו –

א. הסדרת העברת מידע בין גופים ציבוריים בפרק ד׳ לחוק[4] – בעקבות המלצת ועדת קלוגמן[5];

ב. תיקונים בחוק אשר נועדו להבטיח הגנה טובה יותר על המידע המצוי במאגרים וכן הסדרת תחום הדיוור הישיר[6] וזאת בעקבות המלצה של המועצה להגנת הפרטיות.

1.2.2 – תחום מאגרי המידע כנקשר בזכות לפרטיות

חוק הגנת הפרטיות, כנוסחו היום, משלב את הגנת הפרטיות (privacy) ואת ההגנה על מידע המצוי במאגרי מידע (data protection). תחום ההגנה על המידע והשיח הציבורי בנושא זה, הולכים ומתפתחים עם התקדמות הטכנולוגיה והשימוש היומיומי במאגרים האוספים נתונים רבים ושונים על האוכלוסייה. ככל שהטכנולוגיה משתפרת ומאפשרת אגירת נתונים רבים יותר אשר הנגישות אליהן קלה והמידע הנוסף שניתן להפיק מאותם נתונים משתכלל, גובר החשש בנוגע לפגיעה בפרטיות בהקשר למאגרי מידע.

ישנן הגדרות רבות ל״פרטיות״, אשר הידועה שבהן היא ההגדרה של וורן וברנדייס אשר במאמרם הידוע משנת 1890 הגדירו את הפרטיות כ-"The right to be let alone"[7]. סקירה מורחבת על הזכות לפרטיות אשר הוכנה לחברי הצוות על ידי עו״ד יעקב וילון ממחלקת ייעוץ וחקיקה במשרד המשפטים, מצורפת כנספח לדו״ח זה. לצורך הבנת הקשר בין הזכות לפרטיות להגנה על מידע, ברצוננו להביא את הסיווג אותו אימץ ביהמ״ש הקנדי אשר חילק את האינטרסים המצויים בבסיס הזכות לפרטיות, לשלושה סוגים[8] –

1. פרטיות אישית – בהתייחס לגופו של אדם;
2. פרטיות טריטוריאלית – המתייחסת לביתו של אדם ומתחמים פיסיים נוספים;
3. פרטיות המידע – המתייחסת למידע אישי.

ההגנה על פרטיות המידע נועדה לעגן את זכותו של אדם לשלוט במידע המצוי אודותיו אצל גורמים אחרים. ההנחה היא שאי מתן שליטה מסוימת לאדם על המידע המצוי אודותיו, יגרום לכך שהמידע יהיה מופקר ויעשה בו שימוש כראות עיניהם של מי שהניחו ידם על המידע, אשר עניינו של הפרט אינו בהכרח עומד לנגד עיניהם. החלטה להגן על המידע היא הכרעה ערכית בה החברה מאפשרת למושא המידע, גם אם אינו בעל החזקה במידע, לבקר את השימושים שעושים במידע אודותיו ואף לשלוט בהם. מאותן סיבות מדינות המסדירות את תחום ההגנה על המידע נוהגות לקבוע הנחיות בנוגע לאופן ניהול מאגרי מידע הכוללות הגבלות על השימוש במידע המצוי במאגר.

ככל שהטכנולוגיה מתקדמת ואיתה דרכי איסוף המידע, כמו גם השימוש הגובר והולך בשימור מידע בפורמט דיגיטאלי - קטנה יכולתו של מושא המידע לשלוט בשימוש שנעשה במידע אודותיו. יש לתת את הדעת לכך שהקניית זכויות ביחס למידע למושא המידע, והטלת חובות ביחס לשימוש

---

[4] הצעת החוק פורסמה בה״ח התשמ״ג, עמ׳ 176.

[5] ״הוועדה לעניין העברת ידיעות בין גופים ציבוריים, בראשותו של עו״ד חיים קלוגמן, אשר מונתה ביום 17/2/82 על ידי היועץ המשפטי לממשלה דאז, מר יצחק זמיר.

[6] הצעת החוק פורסמה בה״ח התשנ״ד, עמ׳ 148.

[7] Samuel D. Warren & Louis D.Brandies, *The Right to Privacy*,4 Harvard Law Review 193 (1890)

[8] *R v. Dyment*, [1988] 2 S.C.R 417

במידע, עשויה להביא עמה מידה של התערבות באופן הפעילות הרגיל של מחזיק המידע. בהקשר זה יודגש כי למחוקק אין אינטרס להתערב בפעילות גופים פרטיים ככאלה, או להגביל את המגזר הפרטי בפעילותו במישור האזרחי. עם זאת, בשל פערי הכוחות בין בעליהם של מאגרי מידע לבין מושאי המידע, המחוקק הישראלי ראה צורך להתוות כללים והגבלות בניהול מאגרי מידע.

לעניין זה נציין כי הגישה בארה"ב, אשר בחרה להגן על פרטיות המידע בגופים ציבוריים בלבד, ובתחומי פעילות מסוימים ומוגדרים בלבד, שונה מהגישה האירופאית, אשר בחרה להקנות זכויות למושא המידע במידע המצוי אודותיו מבלי להתייחס היכן המידע שמור. החקיקה הישראלית דומה, לעניין זה, להסדר האירופי.

<u>1.2.3 – פרק ד' לחוק הגנת הפרטיות</u>

במקביל לסיום עבודתו של צוות זה, הוקם צוות לבחינת הוראות פרק ד' המסדיר את העברת המידע בין גופים ציבוריים. צוות זה מורכב מנציגים של גופים ציבוריים שונים. מטרת הצוות היא לבחון את ההסדר הקיים מחדש ולייעל את הביקורת והשקיפות בנוגע להעברת מידע בין גופים ציבוריים, וזאת בעקבות הביקורת של השופטת דורנר בבג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**, פ"ד נח(4) 842.

<u>1.3 – הסדרים בשיטות משפט אחרות</u>

במהלך עבודת הצוות, עמדו לנגד עיניו הסדרים דומים במדינות אחרות. ככלל, הצוות בחן את המצב החוקי בקנדה, באיחוד האירופאי ובאירלנד. בנושאים מסוימים, ובמידת הצורך, בחר הצוות להתייחס אף להסדרים ספציפיים במדינות אחרות, כגון לעניין סטנדרטים של אבטחת מידע.

להלן, בקצרה, רקע מקדים על ההסדרים הקיימים אליהם התייחס הצוות במהלך עבודתו -

<u>1.3.1 – קנדה</u>

בקנדה קיימים שני חוקים הרלוונטים לעניין מאגרי מידע: ה- Privacy Act משנת 1983 (להלן – **חוק הפרטיות**) שחל על גופים ציבוריים וה- Personal Information Protection and Electronic Documents Act (להלן - **PIPEDA**) משנת 2001 אשר מטפל בסוגיות שונות הנוגעות למסמכים אלקטרוניים וחל על המגזר הפרטי. החלק הראשון של ה-PIPEDA עוסק ב- Protection of Personal Information in the Private Sector והוא החלק אשר הוראותיו נוגעות, בין היתר, לניהול מאגרי המידע במגזר הפרטי.

מטרתו של חוק הפרטיות הקנדי, כפי שמופיע בסעיף 2 לחוק, היא:

> "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."

מטרתו של החלק ב-PIPEDA העוסק במידע האישי , כפי שמופיע בסעיף 3 לחוק, היא:

> "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

1.3.2 - האיחוד האירופאי

באיחוד האירופי ישנם מספר הסדרים הנוגעים למאגרי מידע, אך המרכזי והבסיסי שביניהם הוא דירקטיבה[9] 95/46/EC[10] אשר התקבלה ב-24/10/95 ועוסקת בהגנה על מידע אישי (Data Protection) (להלן – **הדירקטיבה**). יעדי הדירקטיבה, כפי שמנוסחים בסעיף 1, הם כדלקמן:

> "Object of the Directive
>
> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."

הדירקטיבה אינה חלה על פעילות שמחוץ למסגרת האיחוד האירופי ובכל מקרה על פעולות עיבוד הנוגעות לביטחון הציבור, להגנה, לביטחון (לרבות ביטחונה הכלכלי של המדינה) ולתחום המשפט הפלילי. עם זאת, חוקיהן של מדינות אירופיות רבות המאמצים את הוראות הדירקטיבה לדין המקומי, מוחלים גם על תחומים אלה, תוך קביעת פטורים לעניינים של ביטחון לאומי ואכיפת חוק (לדוגמא סעיפים 28-29 לחוק הגנת מידע הבריטי, ה-Data Protection Act of 1998). כמו כן הדירקטיבה אינה חלה על עיבוד מידע שנעשה במהלך פעילות שטיבה אישי (סעיף 3(2) לדירקטיבה).

---

[9] דירקטיבה היא חקיקה של האיחוד האירופאי. החקיקה מחייבת את מדינות האיחוד בהתאמת הדין המדינתי להוראות הדירקטיבה אולם מותירה בידיהן שיקול דעת מסוים בנוגע לאופן יישום הדירקטיבה בכל מדינה.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

בנוסף לדירקטיבה 95/46/EC, ישנן דירקטיבות נוספות שיש להן נגיעה לעיבוד מידע כגון – דירקטיבה 2002/58/EC העוסקת בהגנה על הפרטיות בתקשורת אלקטרונית[11], דירקטיבה 2004/23/EC המסדירה את תחום השמירה והאגירה של רקמות ותאים אנושיים[12] ועוד.

<u>1.3.3 – אירלנד</u>

החקיקה באירלנד מסדירה את תחום ה- Data Protection עוד משנת 88'. בעקבות הדירקטיבה האירופית, תוקן החוק לאחרונה[13] באופן נרחב (להלן – **חוק הגנת המידע**).

מטרת החוק, כפי שהיא מופיעה בכותרת המורחבת שלו, היא:

> "An Act to give effect to the convention for the protection of individuals with regard to automatic processing of personal data done at Strasbourg on the 28th day of January, 1981, and for that purpose to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. An Act to give effect to directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, for that purpose to amend the data protection act, 1988, and to provide for related matters. "

---

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). דירקטיבה זו החליפה את דירקטיבה 97/66/EC באותו נושא בעקבות ה-11 לספטמבר. לאחרונה אושרה דירקטיבה אשר אומצה כמשלימה לדירקטיבה 2002/58/EC ומסדירה העברת נתוני תקשורת משרותי תקשורת ורשתות תקשורת (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[12] Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells

[13] אפריל 2003

1.4 - מבנה הדו״ח

דו״ח זה יסקור את הנושאים כפי שנדונו בצוות. בראש כל פרק (נושא) תופיע סקירה של המצב הקיים בישראל ושל ההסדר הקיים במדינות שונות. כמו כן, הדו״ח מביא את הדעות המנומקות של הצוות והמלצותיו. דעת מיעוט תצוין רק במקום בו העמדה הייתה משותפת ליותר מחבר יחיד, אולם במקום בו היתה דעת יחיד, יצוין כי ההמלצה היא על דעת מרבית חברי הצוות.

סדר הפרקים בדו״ח מקביל, ככלל, לסדר ההוראות והנושאים כפי שמצויים בחוק עצמו. בסיומו של כל פרק מופיעה המלצת הצוות למשרד המשפטים, כאשר כלל ההמלצות מרוכזות בסיכום לדו״ח. בשל מחלוקות רבות על נוסח ההסדר בחקיקה, ועל מנת לא לעכב את פרסום הדו״ח יתר על המידה, החליט הצוות לפרסם את הדו״ח עם המלצותיו ללא נוסח מוצע - למעט במקום בו ההמלצה נוגעת להגדרה בחוק.

2 - היקף התחולה של פרק ב'

בטרם נדון בהסדר החוקי הרצוי בנושא מאגרי מידע, נבחנו שתי סוגיות ראשוניות:

1. האם יש להגן על תאגידים כנפגעים פוטנציאלים במסגרת הסדרת תחום מאגרי המידע;
2. הסדרת תחום מאגרי המידע שאינם ממוחשבים.

2.1 - תאגיד כנפגע פוטנציאלי

2.1.1 - המצב הקיים

סעיף 3 לחוק הגנת הפרטיות קובע כי:

" "אדם" - לענין סעיפים 2, 7, 13, 14, ו - 25 למעט תאגיד "

בהקשר לתחום מאגרי המידע, החוק הקיים אינו מכיר בזכות העיון[14] וזכות התיקון[15] של תאגיד, בנוסף מאגר שהמידע המצוי בו הוא מידע רק על תאגידים בלבד, אינו "מאגר מידע" כהגדרתו בחוק. נציין כי בהצעת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ו-2005[16] (להלן – **הצעת החוק**) מוצע לתקן את הגדרת אדם כך שיוציא מגדר פרקים ב' ו-ד' בכללותם, את ההגנה על תאגידים כבעלי זכויות בהיותם מושאי המידע. מקור הטעות הוא בכך שעת נוספו הסעיפים הרלוונטיים (17ב, 17ג, 17ו, 17ז, 23א ו-23ב) לא תוקן סעיף 3 בהתאמה.

בדברי ההסבר להצעת החוק נאמר כי –

> "חוק הגנת הפרטיות נועד, ככלל, להגן על הזכות לפרטיות של בני אדם ולא של תאגידים. הדבר בא לידי ביטוי בהגדרה "אדם" שבסעיף 3 לחוק האמור, וכן בפסיקת בתי המשפט. מוצע לתקן את ההגדרה האמורה כך שתחול . . . לגבי הוראות סעיפים 17ב', 17ג', 17ו' ו-17ז' לחוק הגנת הפרטיות, העוסקים במאגרי מידע למטרות דיוור ישיר, והוראות סעיפים 23א' ו-23ב לחוק האמור העוסקים במסירת מידע או ידיעות מאת גופים ציבוריים."

במהלך עבודת הצוות נבחן הצורך בשינוי המצב הקיים אשר בחר שלא לתת הגנה לתאגידים בהיותם מושאי מידע במאגר מידע.

2.1.2 - משפט משווה

בהסדרים אותם בחן הצוות, הגדרת המידע וההגנה על המידע נוגעת לבני אדם בלבד ולא לתאגידים. נדגיש כי נבחנו הסדרים הנוגעים לפרטיות או להגנה על מידע בלבד, ולא הסדרים שהערך המוגן בבסיסם נוגע לסודות מסחריים או הגנה על זכות הקניין.

2.1.2.1 – קנדה

שני החוקים הרלוונטיים בקנדה, חוק הפרטיות וה-PIPEDA, מתייחסים בהגדרת "מידע אישי" (המופיעה בפרק 3.1.2.1 של הדו"ח) ל"individual " – דהיינו לבני אדם בלבד.

---

[14] חוק הגנת הפרטיות, סעיף 13

[15] חוק הגנת הפרטיות, סעיף 14

[16] פורסם בה"ח התשס"ו, עמ' 230.

2.1.2.2 – האיחוד האירופי

הדירקטיבה האירופית מתייחסת בהגדרת מידע אישי ל"natural person" – בני אדם בלבד.

2.1.2.3 – אירלנד

חוק ההגנה על מידע באירלנד מתייחס בהגדרת המידע למונח "living individual" – בני אדם חיים בלבד.

<u>2.1.3 - דעת הרוב</u>

מרבית חברי הצוות סבורים שיש להשאיר את המצב על כנו ממספר טעמים. הראשון בהם הוא כי פרטיות היא חלק מזכויות האדם שמטיבן הן זכויות של בני אדם ולא של כל אישיות משפטית. בהתייחס לזכות לפרטיות, נוסף על הצורך האנושי באינטימיות, זכות זו מבוססת על רעיונות כמו כבוד האדם, האוטונומיה של הרצון החופשי, הצורך במרחב עצמאי (פיסי ווירטואלי) שבו האדם יכול להיות – אם ירצה – לבדו, כדי לפתח את אישיותו וזהותו. רציונאלים אלו אינם תקפים בכל הנוגע לתאגידים.

כאשר מסדירים הגנה על בן אדם כמושא מידע במאגרי מידע, הערך המוגן בבסיס ההסדר הוא הפרטיות. לעומת זאת, בהסדרת הגנה על תאגיד כמושא מידע, הערך המוגן הוא הפגיעה בזכות הקניינית של התאגיד. לפיכך, גם אם ישנן זכויות של התאגיד הדורשות הגנה, חוק הגנת הפרטיות אינו הפלטפורמה עליה רצוי לבסס את אותן הגנות. ערך הקניין עשוי להיות מוגן במערך חוקים ודינים אחר ביניהם דיני הסודות המסחריים כפי שמעוגנים בחוק עוולות מסחריות, תשנ"ט-1999[17], הגנה על מאגרי מידע בהתקיים תנאים מסוימים לפי חוק זכות יוצרים, 1911,[18] חוק המחשבים, האוסר חדירה לחומר מחשב, כללים בדבר חיסיון בנקאי, חיסיון עורך-דין-לקוח, ועוד רשת דינים. הצוות מציין לפניו גם את עמדת ועדת החוקה, חוק ומשפט של הכנסת, שדנה בזכות החוקתית לפרטיות, אגב דיוניה בעיגון הזכות לפרטיות בחוקה (במסגרת הדיונים לקראת הכנתה של "חוקה בהסכמה" במהלך הכנסת ה-16)[19], כאשר הדעה שרווחה בדיון היתה שאין להחיל את ההגנה על הפרטיות על תאגידים.

בעניין זה קיימת הבחנה נוספת - בין התאגיד כאישיות נפרדת לבין בני האדם המרכיבים את התאגיד. העובדה שאיננו מכירים בזכות התאגיד לפרטיות בהקשר למאגרי מידע, איננה שוללת את זכותו של הפרט בתוך התאגיד, להגנה על פרטיותו. לדוגמא, מאגר המרכז נתונים על רווחיהן של חברות, אינו מהווה "מאגר מידע" כהגדרתו לפי סעיף 7 לחוק ועל כן למושאי המידע לא תהיינה זכויות מכוח חוק הגנת הפרטיות לעיין ולתקן את המידע המצוי באותו מאגר. אולם, אין באמור כדי להשליך על הסיווג של מאגר בו מצויים הכנסותיהם של פרטים בתוך תאגיד מסוים, בהתייחס להגדרת "מאגר מידע" בחוק ולהשלכות מכוחו.

לסיום, נציין כי קיים חשש שהחלת פרק ב' גם על תאגידים עלולה להוביל לפרשנות שתגביל את היקף הזכות ותצמצם אותה. החלת הזכות לפרטיות גם על תאגיד מנתקת את הזכות לפרטיות מהקשרה המקורי, ועלולה להביא לעיתים לאבסורד או להקניית חסינויות מופרזות לישויות

---

[17] ס"ח התשנ"ט, עמ' 146.

[18] חא"י, כרך ג', עמ' 2633 .

[19] ראו פרוטוקול ועדת חוקה, חוק ומשפט מיום 22/11/04 פורסם באתר חוקה בהסכמה .

מלאכותיות. לשם איזון עלולים בתי המשפט לצמצם את היקפה של הזכות במקרים שהדבר מתבקש בהקשר של תאגיד, אבל הצמצום יפגע בזכות לפרטיות של בני אדם בשר ודם. ניתן לשקול לקבוע או לחדד את הסייג לגבי תאגיד בעת הגדרת "מידע" או "מידע אישי": הגבלת ההגדרה למידע אודות "אדם שאינו תאגיד".

2.1.4 - דעת המיעוט[20]

לדעת מיעוט חברי הצוות יש להסדיר את תחום מאגרי המידע גם כאשר מושאי המידע הנם תאגידים. עמדה זו מבוססת על מספר נימוקים.
המנדט שניתן לצוות הוא לבחינת ההסדר בנוגע להגנה על מידע ולא להסדרת תחום הפרטיות "הקלאסית". הוראות פרק ב' מנסות להתוות נורמות מחייבות לגבי ניהול מידע תוך תפיסה כי מי שבידו מידע רב, מהווה סיכון בתחום הפרטיות בשל החשש משימוש לרעה במידע המצוי בידו בין אם על ידי אדם מטעמו ובין אם על ידי גורם חיצוני שהצליח לשים ידיו על המידע האגור אצלו.
כמו כן לשיטתם, מכיוון שלא ניתן להפריד בצורה מוחלטת בין התאגיד לבין הפרטים המרכיבים אותו, ממילא פגיעה ב"פרטיות" התאגיד פוגעת גם בפרטיות הפרטים שבו.
אבחנה בין "אדם" ל"תאגיד" מקנה הגנה משפטית שונה שמקורה רק בעובדה שבני אדם בחרו הסדר משפטי מסוים – בחירה שאינה אמורה להיות רלוונטית בהקשר לסוגיה של הגנה על מידע. חברי דעת המיעוט כופרים באבחנה הנוצרת בין פרטיותו של עוסק מסוים שלא התאגד, לבין חברו בעל אותו עיסוק שבחר להתאגד מטעמים אשר ניתן להניח כי אינם נוגעים להגנת הפרטיות, וזאת במיוחד לאור העובדה שתאגידים הם אמצעי הפעולה המקובל בעולם המודרני. למסך ההתאגדות אין רלבנטיות לעניין הערכים המוגנים על ידי חוק הגנת הפרטיות. ההגנה הקניינית נועדה להגן על מידע בעל ערך קנייני, במובחן מנחלת הכלל. ההגנה של דיני הפרטיות נועדה להגן על אינטרס אחר, שהוא שימוש לרעה במידע, גם אם מדובר במידע פומבי שהוא חסר ערך כלכלי כשלעצמו.

2.1.5 – המלצת הצוות

מוצע להשאיר את המצב החוקי על כנו בכפוף לתיקונים המוצעים בהצעת החוק.

[20] עמית אשכנזי, יוספה טפיירו, נחמן ליס ובובי פיינדריך.

2.2 – החלת החוק על מאגרי מידע שאינם ממוחשבים

2.2.1 - המצב הקיים

הגדרת "מאגר מידע" בסעיף 7 לחוק קובעת כי -

> " "מאגר מידע" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב " [ההדגשות שלי – ר.ד]

מבחינת ההסדר הקיים, הוראות פרק ב' אינן חלות על מאגרי מידע שאינם ממוחשבים. הטעם לכך מצוי בדו"ח של ועדת גלס[21], שאת המלצותיה אימץ המחוקק באמצעות חקיקת פרק ב' לחוק הגנת הפרטיות –

> "(א) ... המחשב מגדיל את כושר הקיבול של מאגרי המידע למימדים עצומים ומספק אמצעי איחסון נוחים וקומפקטיים של נתונים הניתנים לשליפה ולהעברה מהירה ...
> (ב) מלבד הסכנה לפגיעה בפרטיות האזרח בעצם הריכוז של כמויות גדולות של מידע אישי במאגר אחד יוצר המחשב סכנות נוספות: המחשב מאפשר גישה למידע ממקומות שונים ומרוחקים ע"י הפעלת מסופים או התחברות לקוים בציוד אלקטרוני; המחשב מאפשר העברת מידע ממערכת נתונים אחת למערכת שניה ובכך יוצר אפשרויות של שילוב נתונים ..." [עמ' 3-4 לדו"ח ועדת גלס]

2.2.2 - משפט משווה

2.2.2.1 - קנדה

חוק הגנת הפרטיות הקנדי מתייחס לאגד של מידע אישי באופן הבא -

> "personal information bank" means a collection or grouping of personal information described in section 10;
> . . . . .
>
> **10.** (1) The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that
> (*a*) has been used, is being used or is available for use for an administrative purpose; or
> (*b*) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
> (2) Subsection (1) does not apply in respect of personal information under the custody or control of the National Archivist of Canada that has been transferred to the National Archivist of Canada by a government institution for archival or historical purposes. "

---

[21] הוועדה למניעת פגיעה באזרח באמצעות מידע המרוכז במחשבים. הדו"ח הוגש בשבט התשמ"א - ינואר 1981

דהיינו, בחוק זה אין אבחנה בין מאגרי מידע ממוחשבים למאגרים שאינם ממוחשבים.

ב-PIPEDA אין התייחסות למאגרי מידע אלא למסמך, לרשומה ("record").

2.2.2.2 – האיחוד האירופי

האיחוד האירופי אינו יוצר אבחנה בין מאגרי מידע ממוחשבים לשאינם ממוחשבים. על פי ההגדרה המופיעה להלן, הדגש שניתן הוא יכולת הנגישות למידע על פי קריטריון מסוים.

> " "personal data filing system" ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis; "

2.2.2.3 - אירלנד

אירלנד בחרה לנסח הגדרת "מאגר מידע" באופן הבא –

> " "Relevant filing system" means any set of information relating to individuals to extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. "

2.2.3 - דעת הרוב

מרבית חברי הצוות סבורים כי הגדרת מאגר מידע צריכה לכלול גם מאגרי מידע שאינם ממוחשבים. אמנם יש להניח כי הסכנה לפגיעה בפרטיות הנובעת ממאגרים ידניים פחותה מהסכנה שבמאגרים ממוחשבים, שכן קשה יותר להצליב את המידע עם מידע אחר ומגבלות המדיום הידני מקשות על הפצת המידע, אולם, אין בכך כדי למנוע את הסכנה שיש במאגרים אלה לזכות לפרטיות.

בנוסף, ההבחנה בין מאגרים ממוחשבים למאגרים שאינם ממוחשבים היא, במידה מסוימת, אבחנה מלאכותית, במיוחד לאור העובדה כי ניתן כיום, בקלות יחסית, להמיר מאגר מידע ממוחשב למאגר מידע ידני ולהפך. טעם נוסף לצורך להחיל את החקיקה גם על מאגרי מידע ידניים, הוא הרצון לצמצם את הפער בין הדין הישראלי לדין האיחוד האירופי.

2.2.4 - דעת המיעוט[22]

מיעוט חברי הצוות סבורים כי אין להרחיב את ההסדר הקיים גם על מאגרי מידע שאינם ממוחשבים.

לשיטתם מידת הפגיעה הנגרמת ממאגרי מידע שאינם ממוחשבים, קטנה בשל חוסר היכולת הטכנית לבצע חיתוכים, הצלבות והעברות מידע. בפועל, תחום מאגרי המידע הלא ממוחשבים ייעלם בעתיד.

2.2.5 - המלצת הצוות

במקום הרישא של הגדרת ״מאגר מידע״ יבוא – **״מאגר מידע״ אוסף של נתוני מידע אישי שניתן לאתר מידע המצוי בו לפי אפיון או חתך מסוים.**

[22] עומר טנא, חיים קלוגמן וחיים רביה

3 - הגדרות

3.1 – הגדרת "מידע"

3.1.1- המצב הקיים

הגדרת "מידע" בסעיף 7 לחוק קובעת כי -

" "מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו ; "

הגדרת המידע כיום הינה הגדרה עמומה אשר מובילה לחוסר בהירות של החוק ולפרשנויות שונות.

3.1.2 - משפט משווה

3.1.2.1 – קנדה

בחוק הפרטיות הקנדי, הגדרת מידע אישי היא כדלקמן -

" "personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing . . ."

החוק ממשיך ומונה דוגמאות למידע אישי כגון מידע על גזע, לאום, חינוך, מצב רפואי ועוד כהנה וכהנה דוגמאות. לאחר מניית מספר דוגמאות למידע אישי, קובעת ההגדרה כי לעניין מספר סעיפים אין להתייחס למידע מסוים כמידע אישי. לדוגמא, מידע מסוים על עובדי ציבור (סעיף 3(f) לחוק הפרטיות), מידע מסוים על מי שהתקשר בחוזה למתן שירותים עם המדינה (סעיף 3(k) לחוק הפרטיות), מידע על הטבה כלכלית שניתנה לאדם (סעיף 3(l) לחוק הפרטיות) ומידע על אדם שנפטר לפני יותר מ-20 שנה (סעיף 3(m) לחוק הפרטיות).

ב-PIPEDA הגדרת מידע אישי מנוסחת באופן הבא –

" "personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."

3.1.2.2 – האיחוד האירופי

האיחוד האירופי מגדיר "מידע אישי" באופן הבא -

"(a)"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or

more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

3.1.2.3 – אירלנד

האירים שינו מעט מההגדרה כפי שנוסחה בדירקטיבה. באירלנד, בשונה מקנדה, מודגש כי מידע מוגדר כמידע אישי רק אם הוא נוגע לאדם אשר עדיין נמצא בין החיים. להלן ההגדרה כפי שהיא מופיעה בחוק הגנת המידע באירלנד -

> " "personal data" means data relating to a living individual who is or can be identified either from the data or from the data conjunction with other information that is in, or is likely to come into, the possession of the data controller"

<u>3.1.3 – הסכמה כללית</u>

בעניין זה הייתה הסכמה כללית של הצוות כי יש ליצור הגדרה ברורה הכוללת את כל המידע אודות אדם. מידע אודות אדם עלול לפגוע בפרטיותו רק כאשר ניתן לזהות את אותו אדם אודותיו המידע. לפיכך המלצת הצוות היא להוסיף כי הגדרת מידע רלוונטית רק למידע אודות אדם מזוהה או הניתן לזיהוי (לדוגמא על בסיס מספר מזהה).

לעניין זה מבקש הצוות להפנות את תשומת לב משרד המשפטים לכך שהחוק נוקט מונחים שונים בהקשרים דומים, דבר הגורם לאי אחידות בדברי החקיקה. לדוגמא, "ענייניו הפרטיים" צנעת חייו האישיים", "ידיעות הנוגעות לחייו האישיים", "מידע" ו"מידע רגיש". השימוש במונחים שונים לכוונות דומות גורם לאי בהירות פרשנית. עם זאת, מכיוון שהצוות לא דן בהוראות החוק המעגנות את ה"פרטיות הקלאסית" (לרבות פרק א' לחוק) ולא נבחנו המשמעויות של שינוי מונחים אלו בחקיקה, מוצע כי בעתיד תינתן הדעת על שימוש במונחים אחידים בחוק.

<u>3.1.4 - המלצת הצוות</u>

1. מוצע לשנות את הגדרת "מידע" באופן הבא -

"מידע אישי" כל מידע אודות אדם מזוהה או הניתן לזיהוי באמצעים סבירים;

2. מומלץ כי בעתיד ייבחנו איחוד המונחים המצביעים על "פרטיות" בחוק.

3.2 – הגדרת "מידע רגיש"

3.2.1 - המצב הקיים

הגדרת "מידע רגיש" בסעיף 7 לחוק קובעת כי -

" "מידע רגיש" -

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש; "

כיום, האבחנה בין "מידע" ל"מידע רגיש" הוא בכך שהגדרת מידע כוללת גם את מעמדו האישי של אדם ואת הכשרתו המקצועית. האבחנה השולית בין שני מושגים אלו גרמה לכך שבפועל אין משמעות רבה לאבחנה בין שני המושגים. גם כאן, כמו בהגדרת "מידע", ההגדרה עמומה ואינה מאפשרת בהירות של החוק.

נציין כי שר המשפטים לא השתמש בסמכותו להרחיב את הגדרת המידע הרגיש.

3.2.2 - משפט משווה

3.2.2.1 – קנדה

בקנדה, בשני החוקים הרלוונטים, אין התייחסות בקטגוריה נפרדת מהגדרת מידע הרגילה, למידע אישי שניתן להגדירו כ"מידע רגיש".

3.2.2.2 – האיחוד האירופי

בסעיף 8 לדירקטיבה האירופית נאסר, לכאורה, לעבד מידע הנוגע לאחד מסוגי המידע המנויים בסעיף, שניתן להתייחס אליהם כמידע רגיש –

" Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. "

עם זאת, יש להדגיש כי הסעיף מונה סייגים רחבים לאיסור לעבד "מידע רגיש" כגון כאשר ישנה הסכמה של מושא המידע (סעיף 8(2)(a) לדירקטיבה); כאשר העיבוד מתבצע במהלך הפעילות הלגיטימית של גוף שאינו למטרות רווח ומושא המידע הוא חבר הגוף וזאת בתנאי שהמידע לא יועבר לצדדים שלישיים ללא הסכמתו (סעיף 8(2)(d) לדירקטיבה); במקרה בו המידע פורסם על ידי מושא המידע וכן במקרה בו המידע נחוץ לצורך ניהול הליך משפטי (סעיף 8(2)(e) לדירקטיבה); כאשר המידע נדרש לצרכים רפואיים (סעיף 8(3) לדירקטיבה). כמו כן ישנה אפשרות כי המדינות יקבעו חריגים נוספים על אלו שנקבעו מטעמים של "אינטרס ציבורי" וזאת לפי דין או על פי החלטת הרשות המפקחת (סעיף 8(4) לדירקטיבה), וכן ניתן לנהל מרשם פלילי בתנאים מסוימים (סעיף 8(5) לדירקטיבה).

3.2.2.3 - אירלנד

באירלנד בחרו ליישם את הדירקטיבה על ידי ניסוח הגדרת מידע אישי כדלקמן –

> " Sensitive personal data means personal data as to –
> (a) the racial or ethnic origin, the political opinions, religious or philosophical beliefs of the data subject,
> (b) whether the data subject is a member of a trade-union,
> (c) the physical or mental health or condition or sexual life of the data subject,
> (d) the commission or alleged commission of any offence by the data subject, or
> (e) any proceeding for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings."

<u>3.2.3 – דעת הרוב</u>

נציין כי בנושא זה היו דיונים מרובים בהם ניסה הצוות להגיע להגדרה של "מידע רגיש". שני הקשיים העיקריים של הצוות נבעו מרצונו לנסח הגדרה חדה וברורה וכן מחשש כי ניסוח מחודש של ההגדרה עלול לגרום לפרשנות אשר תגרום לבעל מאגרי להקל ראש בנוגע למידע שהוחלט לא להכלילו במסגרת הגדרת "מידע רגיש".

בסיכומו של יום מרבית חברי הצוות סבורים כי מכיוון שלהגדרת "מידע רגיש" יש נפקות רק לעניין רישום מאגר המידע, הצוות ימליץ כי בהוראה המחייבת רישום מאגרי מידע ימנו סוגי המידע שהכללתם במאגר מידע יחייבו את בעל המאגר ברישומו. לשיטתם, בית המשפט בבואו לדון בהפרה של הזכות לפרטיות, יביא בחשבון את סוג המידע בו נעשה שימוש אסור על מנת להכריע בעונשו של העבריין. לפיכך אין צורך בקביעת מדרג בין "מידע" ל"מידע רגיש", למעט לצורך חובת הרישום.

חברי הצוות מנו את סוגי המידע אשר לדעתם אחזקתם יחייבו את בעל המאגר לרשום את המאגר בפנקס רשם מאגרי המידע, וזאת על מנת לאפשר ביקורת על בעלי אותם מאגרים. לדעת הצוות יש לחייב ברישום בעלי מאגרי מידע המחזיקים במידע כמפורט להלן -

1. מידע רפואי ונפשי;
2. מידע גנטי;
3. מידע ביומטרי[23];
4. מידע על צנעת חייו האישיים של אדם[24];
5. מידע אודות עברו הפלילי של אדם;
6. מידע אודות דעותיו הפוליטיות ואמונותיו של אדם.

---

[23] יש להבהיר בנוסח החקיקה כי "מידע ביומטרי" הינו מאפיין פיזיולוגי או ביולוגי אנושי ייחודי אשר ניתן למדידה וניתן לעשות בו שימוש לשם זיהוי אוטומטי או סמי-אוטומטי של בני אדם. לדוגמא – טביעות אצבע, דנ"א, טביעת קשתית העין וכד'.

[24] הכוונה במינוח זה היא מידע הנוגע להעדפותיו, להרגליו ומעשיו המיניים של אדם.

3.2.4 - דעת מיעוט[25]

לדעת מיעוט חברי הצוות יש להגדיר בחוק סוגי מידע שייחשבו כ״מידע רגיש״ ולהחמיר בנורמות שיוטלו על מי שמחזיק, מנהל או בעל מאגר מידע רגיש. לדוגמא, חומרת העבירה וחומרת הסנקציה הפלילית במקרה מסוים צריכות להיגזר מרגישותו של המידע באמצעותו התבצעה ההפרה. כמו כן מציעים חברי דעת המיעוט כי יוטלו על גוף המחזיק מידע רגיש איסור לאסוף מידע שאינו רלוונטי למטרות לשמן הוקם המאגר וכן בעלי המאגר יידרשו למחוק מידע עודף המצוי במאגר.

חשיבות נוספת, לדעתם, להגדרת ״מידע רגיש״ היא פרשנית - היקף החובות שבחוק ויישומן הקונקרטי תלוי בנסיבות העניין, ואחת מהנסיבות העניין היא היותו של המידע ״רגיש״. כך, למשל, כאשר בית המשפט יצטרך לקבוע מהם אמצעי האבטחה שהיה על בעל מאגר סביר להנהיג, הוא יביא בחשבון, בין היתר, את העובדה שהמאגר מכיל מידע שהמחוקק ראה כ״רגיש״.

3.2.5 - המלצת הצוות

מוצע למחוק את הגדרת ״מידע רגיש״ ובמקומה למנות את סוג המידע שאגירתו במאגר מידע יחייב את רישום המאגר בפנקס המתנהל אצל רשם מאגרי המידע.

[25] עמית אשכנזי, עומר טנא ואבנר פינצ׳וק

4 - חובת רישום מאגרי מידע

4.1 – חובת הרישום

4.1.1 - המצב הקיים

מאגר מידע חייב ברישום אם התקיימו בו אחד מהתנאים הבאים, למעט אם יש בו רק מידע שפורסם לרבים או הועמד לעיון הרבים על פי דין (סעיפים 8(ג)-(ד) לחוק):

1. מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000 (סעיף 8(ג)(1) לחוק);
2. יש במאגר מידע רגיש (סעיף 8(ג)(2) לחוק);
3. המאגר כולל מידע על אנשים והמידע לא נמסר על ידם, מטעמם או בהסכמתם (סעיף 8(ג)(3) לחוק);
4. המאגר הוא של גוף ציבורי (סעיף 8(ג)(4) לחוק);
5. המאגר משמש לשירותי דיוור ישיר (סעיף 8(ג)(5) לחוק);

עם זאת, מוקנית סמכות לרשם להורות על קיום חובת רישום לגבי מאגר הפטור מחובת רישום, מטעמים מיוחדים שיירשמו (סעיף 8(ה) לחוק).

4.1.2 - משפט משווה

4.1.2.1 – קנדה

בקנדה, בכל הנוגע למאגרי מידע של גופים במגזר הפרטי, אין הסדר הדומה להסדר הרישום המצוי בחוק הישראלי. לעומת זאת, חוק הפרטיות הקנדי עוסק רק במידע אישי המצוי בידי רשויות ("personal information banks"), המקיים שני תנאים –

1. נעשה בו שימוש (בעבר או בהווה) או שהוא נגיש לשימוש למטרות מנהליות וכן,
2. המידע מאורגן כך שניתן לאתר אותו על פי נתון מזהה (סעיף 10 לחוק הפרטיות).

סעיף 11 לאותו חוק מחייב את השר הממונה לפרסם אחת לתקופה, ולא פחות מאחת לשנה, אינדקס בו יופיעו רשימת המאגרים הממשלתיים ולגבי כל מאגר יפורסם –

- זהות ותאור המאגר (סעיף 11(a)(1) לחוק הפרטיות);
- איזו רשות שולטת במאגר (סעיף 11(a)(2) לחוק הפרטיות);
- דרכי ההתקשרות עם הפקיד אליו ניתן להגיש בקשות בנוגע למידע המצוי במאגר (סעיף 11(a)(3) לחוק הפרטיות);
- הצהרה על מטרות המאגר ואופן השימוש בו (סעיף 11(a)(4) לחוק הפרטיות);
- התייחסות להוראות הנוגעות למחיקת מידע (סעיף 11(a)(5) לחוק הפרטיות);
- אינדיקציה לכך שלמאגר יש פטורים מהוראות חוק מסוימות (סעיף 11(a)(6)).

4.1.2.2 – האיחוד האירופי

הדירקטיבה האירופית יוצרת הסדר של מתן הודעה (notification) הדומה, כעקרון, להסדר הרישום בארץ. "ההודעה" צריכה להיות מועברת בטרם ביצוע פעולה הנוגעת לעיבוד מידע אוטומטי (סעיף 18(1) לדירקטיבה). הדירקטיבה מאפשרת למדינות לפטור ממתן הודעה באחד מהמקרים הבאים:

1. במקרה של עיבוד מידע שלא סביר, בהתחשב בנתונים המעובדים, כי ייפגעו זכויותיהם של מושאי המידע (סעיף 18(2) לדירקטיבה);
2. במקום בו בעל המאגר, בהתאם לחקיקה המקומית, ממנה אחראי הגנת מידע (personal data protection official) אשר יבטיח, תוך שמירה על מעמדו העצמאי, כי המאגר מנוהל על פי הסטנדרטים שנקבעו בחקיקה המדינתית בהתאם לדירקטיבה, ינהל את הרישום על פעולות עיבוד המידע המבוצעות על ידי בעל המאגר ויבטיח כי ישנה סבירות נמוכה שזכויות מושאי המידע יפגעו מעיבוד המידע (סעיף 18(2) לדירקטיבה);
3. מאגר מידע המקיים רישום שמטרתו העברת מידע לציבור ועל כן פתוח לעיונו (סעיף 18(3) לדירקטיבה).

לפי הדירקטיבה, "ההודעה" תכלול לכל הפחות את הפרטים הבאים:

- שם וכתובתו של בעל המאגר או נציגו (סעיף 19(1)(a) לדירקטיבה);
- מטרות המאגר (סעיף 19(1)(b) לדירקטיבה);
- תיאור קטגוריות המידע (סעיף 19(1)(c) לדירקטיבה);
- מי יהיה חשוף למידע (סעיף 19(1)(d) לדירקטיבה);
- העברת מידע למדינות שלישיות (סעיף 19(1)(e) לדירקטיבה);
- תיאור כללי לגבי אבטחת המידע (סעיף 19(1)(f) לדירקטיבה).

4.1.2.3 – אירלנד

באירלנד ניתן פטור מרישום במקרים הבאים:

1. כאשר המרשמים פתוחים לעיון הציבור (סעיף 16(1)(1) לחוק הגנת המידע);
2. אם מאגר המידע אינו ממוחשב (סעיף קטן 16(1)(2) לחוק הגנת המידע);
3. במקרה בו העיבוד מתבצע במהלך הפעילות הלגיטימית של גוף שאינו למטרות רווח ומושא המידע הוא חבר הגוף או מישהו שהוא בקשר קבוע עם הארגון (סעיף 16(1)(b) לחוק הגנת המידע).

ההסדר בחוק הגנת המידע מפרט את אופן ניהול המרשם והיותו פתוח לעיון הציבור (סעיף 18 לחוק הגנת המידע). באירלנד חל איסור להחזיק מאגר החייב ברישום עד שבוצע רישום כאמור (סעיף 19(1) לחוק הגנת המידע), והפרת האיסור מהווה עבירה פלילית (סעיף 19(6) לחוק הגנת המידע). כמו כן, החוק מדגיש כי בעל המאגר מחויב לפעול בהתאם לאופן בו תואר המאגר במרשם (סעיף 19(2) לחוק הגנת המידע).

4.1.3 - דעת הרוב

מרבית חברי הצוות סבורים כי יש לצמצם את חובת הרישום כך שתחול בהתקיים אחת מהנסיבות הבאות -

1. כאשר בעל המאגר "סוחר" במידע שברשותו (מאגר המשמש לשרותי דיוור ישיר);
2. כאשר המאגר כולל מידע בעל רגישות מיוחדת, כמוצע בפרק 3.2 לדו"ח זה[26], כיוון שיש אינטרס מוגבר של הציבור לקבל פרטים אודות מאגרים אלו.

לשיטתם, ההסדר הקיים היום אינו מעשי. הגדרת "מאגר מידע" רחבה ועמומה ומובילה לחוסר ודאות בנוגע לחובת הרישום. כמו כן, חובת רישום רחבה כפי שקיימת היום בדין הישראלי, מובילה לכך שיחידת הרשם עוסקת בטפל (רישום) ולא בעיקר (פיקוח). בפועל ההערכה היא כי רק כ-2% ממאגרי המידע רשומים - כך שישנה זילות של הוראות החוק בנוגע לרישום המאגרים.

בנוסף, חוסר היכולת לאכוף את חובת הרישום, מוביל להפליית בעלי המאגרים הממלאים חובתם כדין בין היתר בכך שנדרש מהם תשלום שנתי עבור הרישום.

4.1.4 - דעת מיעוט[27]

לדעת מיעוט חברי הצוות, אין לצמצם את חובת הרישום מכפי שהיא מוגדרת כיום. לשיטתם, רישום המאגרים מהווה כלי עזר לבעלי המאגר לבחון אם הם עומדים בדרישות החוק. הדבר מתבצע היות שבעלי המאגר, עת הם נדרשים לשלם את האגרה התקופתית, בוחנים את רישומם בפנקס והאופן בו הם תיארו את פעילות מאגר המידע שבבעלותם. כמו כן, הרישום נדרש לצורך פעילות הפיקוח בכך שהוא ממפה את מאגרי המידע המצויים בידי הרשויות והציבור.

לדעתם, מאגר מידע הוא נכס שמשרת את בעליו ומסב לו תועלות כלכליות ואחרות. כיוון שנכס זה והשימוש בו מייצרים גם סכנות חברתיות, יש צורך לפקח עליהם. מי שצריכים לשאת בעלויות הרגולציה הם בעלי הנכס והנהנים הישירים ממנו ולא הציבור בכללותו. על כן יש מקום לרישום כל מאגר ולגביית אגרת רישום שנתית. גובה האגרה צריך להיות בהתאם לגודל האיום שמייצר המאגר על הפרטיות, דהיינו פונקציה של גודל המאגר, רגישות המידע שבו, השימושים שעושים בו, ועוד.

---

[26] המלצת הצוות בסעיף 3.2 היא הגדרת "מידע רגיש" תימחק, ובמקומה יימנו סוגי המידע שאגירתם מחייבת רישום בפנקס מאגרי המידע. חובת הרישום תחול על מאגרים הכוללים מידע רפואי ונפשי, מידע גנטי, מידע ביומטרי, מידע על צנעת חייו האישיים של אדם, מידע אודות עברו הפלילי של אדם ומידע אודות דעותיו הפוליטיות ואמונותיו של אדם.

[27] יוספה טפיירו, נחמן ליס, בובי פיינדריך, אבנר פינצ'וק

<u>4.1.5 – סמכות רשם מאגרי המידע לצמצם או להרחיב את החובה</u>

4.1.5.1 – מרבית חברי הצוות[28]

ככל שהפטור או החיוב הוא על פי סוג המאגר (הוראה נורמטיבית) – הסמכות תהיה נתונה לשר, ככל שהפטור או החיוב הוא בהתייחס למאגר מסוים (הוראה אישית) – הסמכות תהא נתונה לרשם.

<u>4.1.6 – המלצת הצוות</u>

מוצע –

1. לצמצם את חובת הרישום כך שתחול בהתקיים אחת מהנסיבות הבאות -

א. כאשר בעל המאגר "סוחר" במידע שברשותו;

ב. כאשר המאגר כולל מידע רגיש.

2. להרחיב את סעיף 8(ה) כך שלרשם תהיה סמכות גם לחייב מאגר ברישום, על אף שהוא פטור;

3. להוסיף הוראה לפיה שר המשפטים יהיה רשאי להורות לחייב או לפטור סוג מאגרים מסוים מרישום.

[28] למעט חיים רביה

5 - סמכויות רשם מאגרי מידע

5.1 – סמכויות הרשם

5.1.1 - המצב הקיים

החוק הקיים מונה מספר סמכויות של הרשם בעניינים הבאים:

1. רישום מאגרי מידע (סעיפים 10(א)-(ב3));
2. פיקוח על הוראות החוק בעניין מאגרי מידע (סעיף 10(ג));
3. היות הרשם ראש יחידת הפיקוח ומינוי מפקחים על ידו (סעיף 10(ה));
4. סמכויות פיקוח (סעיף 10(ה1));
5. סמכות לבטל רישום של מאגר או להתלות תוקפו אם הופרו הוראות החקיקה על ידי מחזיק או בעל המאגר (סעיף 10(ו));
6. ניהול פנקס מאגרי המידע (סעיף12).

כמו כן החוק קובע כי הרשם יכין, אחת לשנה, דו"ח על פעולות האכיפה והפיקוח שיוגש לועדת חוקה, חוק ומשפט על ידי המועצה להגנת הפרטיות (סעיף 10א).

5.1.2 - משפט משווה

5.1.2.1 – קנדה

חוק הפרטיות הקנדי מעגן את מעמדו העצמאי של נציב הפרטיות (privacy commissioner) הממונה באופן אישי לאחר קבלת אישורו של הסנאט ושל בית הנבחרים. כהונתו נמשכת 7 שנים והוא יכול להתמנות לכהונה נוספת אחת בלבד (סעיף 53 לחוק הפרטיות).

בחוק, מלבד הסדרת סמכויותיו של הנציב, ישנו פירוט לגבי תנאי העסקתו, העובדה שניתן למנות לתפקיד גם מי שפועל כנציב הממונה על חופש המידע, התייחסות למינוי עוזרים וצוות לנציב, חובת הסודיות וחריגיה, וחיסיון החל על המידע שנאסף על ידי עובדי הנציבות מפני כל הליך משפטי למעט הליך המתנהל לפי אותו חוק.

מלבד נושאים אלו, החוק מציין כי תפקידו של הנציב הוא להוציא לפועל מחקרים שיוטלו עליו על ידי שר המשפטים ועליו לדווח לשר על תוצאות המחקרים מפעם לפעם. המחקרים יתבצעו על ידי הנציב באחד מהנושאים הבאים (סעיף 60 לחוק הפרטיות) –

א. עניינים הנוגעים לפרטיותם של אנשים;

ב. הרחבת זכויות מושאי המידע בנוגע למידע אודותם;

ג. התייחסות לאיסוף, שמירה, מחיקה, שימוש או חשיפה של מידע מלבד בנוגע למוסדות ממשלתיים המצויים תחת סמכותו החוקית של הפרלמנט.

ה-PIPEDA, הממנה את נציב הפרטיות כאחראי גם על מילוי הוראות חוק זה, מקנה לנציב סמכויות רבות נוספות והן -

1. קבלת תלונות וביצוע חקירות, במידת הצורך, בנושא התלונה (סעיף 11 ל-PIPEDA);

2. סמכויות חקירה ביניהן: זימון עדים, חיפוש בחצרים של ארגונים ותפיסה (סעיף 12 ל-PIPEDA);
3. הגשת דו"ח על החקירה תוך שנה מהגשת התלונה למתלונן ולחברה בה נערכה החקירה וזאת למעט במקרים חריגים (סעיף 13 ל-PIPEDA);
4. ביצוע חקירות יזומות כאשר מתעורר חשד כי ארגון מסוים אינו ממלא אחר הוראות החוק (סעיף 18 ל-PIPEDA). והעברת דו"ח החקירה לארגון בתוספת המלצות לתיקון הליקויים (סעיף 19 ל-PIPEDA);
5. פיתוח והעברת מידע במטרה לעודד את הבנת הציבור לגבי הפרק הראשון[29] של ה-PIPEDA (סעיף 24(a) ל-PIPEDA);
6. ביצוע ופרסום מחקרים הנוגעים לאבטחת מידע אישי כולל מחקרים שמתבקשים על ידי שר התעשייה (סעיף 24(b) ל-PIPEDA);
7. עידוד ארגונים לפתח מדיניות ופרקטיקה מפותחות על מנת לעמוד בדרישת הוראות החוק (סעיף 24(c) ל-PIPEDA);
8. קידום, בכל דרך הנראית לנציב, מטרות הפרק הראשון ל-PIPEDA (סעיף 24(d) ל-PIPEDA);
9. בסוף כל שנה יגיש הנציב לפרלמנט דו"ח בנוגע ליישום הוראות אותו פרק, התקדמות חקיקה מתאימה בפרובינציות ויישום אותה חקיקה (סעיף 25 ל-PIPEDA).

5.1.2.2 – האיחוד האירופי

הדירקטיבה האירופית קובעת כי כל מדינה צריכה למנות לפחות רשות אחת שתהיה אחראית על יישום הדירקטיבה. אותן רשויות צריכות לפעול תוך עצמאות מוחלטת (סעיף 28(1) לדירקטיבה); על המדינות להבטיח כי בקביעת תקנות והנחיות מנהליות, יתייעצו עם אותן רשויות (סעיף 28(2) לדירקטיבה). כמו כן, קובעת הדירקטיבה כי לאותן רשויות יוקנו הסמכויות הבאות (סעיף 28(3) לדירקטיבה):

1. סמכויות חקירה;
2. מתן סמכויות אפקטיביות ל"התערבות" (intervention) של אותה רשות;
3. סמכות להתערב בהליכים משפטיים בנוגע להפרת הדירקטיבה או העברת המידע לרשות השופטת.

בנוסף, נקבע כי אותן רשויות יקבלו ויבררו תלונות הנוגעות לתחום טיפולן (סעיף 28(4) לדירקטיבה) ויפרסמו דו"ח פומבי על פעולותיהן באופן קבוע (סעיף 28(5) לדירקטיבה). הרשויות במדינות השונות נדרשות לשתף פעולה זו עם זו (סעיף 28(6) לדירקטיבה).

לסיום, קובעת הדירקטיבה כי על עובדי הרשויות, גם לאחר פרישתן, יחולו חובות סודיות על מידע שהגיע לידיהם במהלך עבודתם ברשות (סעיף 28(7) לדירקטיבה).

---

[29] שהוא החלק העוסק בהגנה על מידע אישי בסקטור הפרטי.

בפועל הוקמו נציבויות לעניין פרטיות והגנת מידע בכל מדינות האיחוד הכפופות להחלטות הנציבות בבריסל. הנציבויות משתפות פעולה ביניהן באמצעות "ועדת סעיף 29" שהוקמה מכוח הדירקטיבה ופועלת באופן עצמאי במטרה לתת ייעוץ למנגנון האיחוד האירופי בנושאים בהם עוסקת הדירקטיבה.

5.1.2.3 - אירלנד

נוסף על דרישות הדירקטיבה, אליהן מפנה החוק האירי, נקבעו מספר הוראות נוספות הנוגעות לסמכותו של הנציב באירלנד –

1. הנציב יבצע מטלות נוספות הנוגעות להגנת מידע שהטיל עליו השר (סעיף 9(1D) לחוק הגנת המידע);
2. הנציב רשאי להורות לבעלי מאגרי מידע לפעול באופן מסוים, כמפורט בסעיף 10 לחוק, ובכלל זה גם לתת הוראות הנוגעות לחסימתו או מחיקתו של מידע מסוים;
3. לנציב סמכויות מיוחדות לפעול כאשר מתבצע עיבוד מידע שלדעת הנציב סביר שיגרום לנזק או מתח ניכר למושאי מידע או שעלול להשפיע באופן משמעותי בזכויות ובחירויות של מושאי המידע (סעיף A12 לחוק הגנת המידע);
4. הנציב יעודד ארגוני סחר וגופים אחרים המאגדים בתוכם בעלי מאגרי מידע מסוג מסוים, לפתח מדיניות העולה בקנה אחד עם הוראות החוק (סעיף 13 לחוק הגנת המידע).

<u>5.1.3 - קביעת הנחיות</u>

כל חברי הצוות סבורים שחובתו של הרשם לקבוע הנחיות בנושאים עליהם הוא אמון, במטרה להבהיר את חובותיהם של העוסקים בתחום ולכוון את התנהגותם בהתאם לנורמות פעולה ראויות. ההנחיות האמורות נדרשות בשל הדינאמיות והמומחיות המאפיינים תחום זה.
עם זאת, חברי הצוות נחלקו בנוגע לצורך בהיוועצות עם גורם נוסף בטרם ההנחיות יפורסמו.

5.1.3.1 – עמדות שונות בנוגע לחובת ההיוועצות של הרשם

5.1.3.1.1 – עצמאות הרשם בקביעת הנחיות[30]

לדעת מספר חברי הצוות אנו דנים בהנחיות, שאינן תקנות, שנועדו לקבוע נורמות ראויות ודינאמיות בתחום מאגרי המידע. קביעת הנחיות כאמור לא נועדה לגרוע מסמכותו של השר לקבוע תקנות בהתאם לחוק על מנת לעגן נורמה כללית ומחייבת, במידת הצורך. היות שלרשם מאגרי המידע יש שיקול דעת עצמאי והמועצה להגנת הפרטיות, אמורה להוות גוף המייעץ לשר כפי שמוצע בסעיף 6.1 להלן, אין סיבה להכפיף את ההנחיות לאישור המועצה או להתייעצות עמה.

---

[30] עמית אשכנזי, רבקי דב"ש, עומר טנא ונחמן ליס

5.1.3.1.2 – קביעת הנחיות תוך חובת היוועצות[31]

לדעת מספר חברי צוות יש לקבוע חובת היוועצות עם המועצה להגנת הפרטיות בטרם ייכנסו הנחיות הרשם לתוקף. הצורך בכך הוא קביעת מנגנון מבקר או מפקח לרשם בקביעת הנחיותיו וזאת על ידי הגוף אשר צבר מומחיות בתחום הגנת הפרטיות וחבריו מייצגים אינטרסים שונים.

5.1.4 – סמכויות פיקוח

לדעת כל חברי הצוות יש לתת לרשם סמכויות פיקוח בדומה לסמכויות אשר מוקנות לו בחוק הקיים.

5.1.5 – אמצעי אכיפה נוספים

כל חברי הצוות סבורים שיש להוסיף לרשם סמכות לתת צווים אישיים כמפורט בפרק 7.4 להלן.

5.1.6 – תחום סמכויותיו של הרשם

הצוות בחן האם יש להרחיב את תחום סמכויותיו של רשם מאגרי המידע גם לאכיפת ההסדר של הגנת הפרטיות הקלאסית הקיים בחוק. לדעת מרבית חברי הצוות[32] אין להרחיב את סמכויותיו של הרשם ממספר טעמים: מלבד העובדה כי לצוות לא היה מנדט לבחון את ההגנה על הפרטיות הקלאסית, וממילא לא נבחנו ההשלכות שיש להחלטה כי הרשם יהיה אחראי גם על האכיפה בתחום זה, אנו סבורים כי תחום מאגרי המידע דורש מומחיות מיוחדת שאינה רלוונטית, בהכרח, להגנה על הפרטיות הקלאסית. כמו כן, בפרטיות הקלאסית יש אמצעי אכיפה יעילים בידי הפרט, כגון קובלנה פלילית או תביעה אזרחית, אשר בהפרות בתחום מאגרי המידע פחות יעילים מסיבות שונות. לדוגמא, המוטיבציה של אדם בודד - אשר נגרם לו נזק מזערי באופן יחסי - לפעול כנגד בעל המאגר פחותה, ולפיכך בתחום זה יש צורך בפיקוח של גורם ציבורי כגון הרשם.

לסיום, לדעת חלק מחברי הצוות, בהעדר נציבות לזכויות אדם הפועלת להגן על מכלול הזכויות הבסיסיות, אין מקום לקדם את הזכות לפרטיות על פני זכויות אחרות באמצעות הקמת מנגנון ייחודי לאכיפת הזכות לפרטיות.

5.1.7 - מעמד רשם מאגרי המידע

בקרב חברי הצוות שררה הסכמה כללית בדבר הצורך בחיזוק מעמדו העצמאי של הרשם. ההליך הפלילי, המהווה כיום את הסנקציה העיקרית בחוק הגנת הפרטיות, אינו אפקטיבי, במרבית המקרים, בתחום מאגרי המידע. מכאן כי הקניית סמכויות אכיפה מגוונות לרשם מאגרי המידע, ללא תלות בגורמי אכיפה נוספים, תאפשר לרשם לפעול לאכיפת הוראות החוק עליהן הוא מופקד באופן יעיל ומרתיע יותר. במסגרת חיזוק מעמדו של הרשם והרחבת סמכויותיו, מציע הצוות למחוקק להשתמש במונח "הממונה על מאגרי המידע" במקום "רשם מאגרי המידע".

עם זאת, חברי הצוות חלקו בשאלת הצורך בעיגון מעמדו העצמאי של הרשם כך שתינתן לו סמכות להתייצב באופן עצמאי בבית המשפט.

---

[31] מיכאל בירנהק, אבנר פינצ'וק, חיים רביה

[32] למעט נחמן ליס

5.1.7.1 – דעת הרוב

לדעת מרבית חברי הצוות יש חשיבות, בשל ניגודי אינטרסים אפשריים, לתת לרשם עצמאות בתוך השרות הציבורי. מכיוון שבידי הגופים הציבוריים יש מספר מאגרי מידע בעלי רגישות הן בשל היקף המידע המצוי בהם והן בשל סיווגו, ייתכן כי העמדה שתוצג על ידי היועץ המשפטי לממשלה לא תשקף בהכרח את העמדה המגנה על הפרטיות במידע אלא את האינטרסים של המדינה בנושא. לשיטת מרבית חברי הצוות רשם מאגרי המידע צריך להיות נאמן פרטיות וזאת לעומת היועץ המשפטי לממשלה אשר צריך לבצע איזון בין הזכות לפרטיות לאינטרסים וצרכים של הרשויות השונות. אם לא תוקנה עצמאות לרשם, המשמעות היא שההכרעה והאיזון בין האינטרס של הרשות לבין הגנת הפרטיות יעשו בתוך הרשות המבצעת - על ידי היועץ המשפטי.

בנוסף, כדי להתאים את המצב המשפטי בישראל לסטנדרט האירופי, יש חשיבות בהגברת עצמאות הרשם, לצד הגברת אמצעי הפיקוח על מינויו, פעולתו, במסגרת האיזונים שבין הרשויות השונות.

5.1.7.2 – דעת המיעוט[33]

לדעת מיעוט חברי הצוות עמדתו של רשם מאגרי המידע יכולה לבוא לידי ביטוי בהליכים משפטיים באמצעות הסמכות המוקנית ליועץ המשפטי לממשלה להתייצב בהליך משפטי שלדעתו יש בה עניין ציבורי[34]. כלומר, במידה שרשם מאגרי המידע, ככל ממלא תפקיד אחר בשרות הציבורי, סבור כי יש עניין ציבורי בגינו יש לשקול התייצבות יועץ, באפשרותו לפנות ליועץ המשפטי לממשלה ולבקש התייצבות כאמור כפי שנעשה בע״א 1949/03 **רוטר נ׳ מכון אדם**.

לעניין התאמת הדין הישראלי לסטנדרט האירופי, חברי המיעוט סבורים כי בבואנו לאמץ עקרונותיו של משפט זר, יש לתת את הדעת, בין היתר, לאופן בו הרשות המבצעת מאורגנת בישראל, לאפשרויות של רשויות המדינה - כפי שהן מעוגנות בדין הקיים - להביא את עמדתן בפני בית המשפט וכן למעמדו, לתפקידו ולסמכויותיו של היועץ המשפטי לממשלה.

לשיטתם, העובדה שהרשם כפוף, במסגרת עקרונות המשפט המנהלי הכללים, ליועץ המשפטי לממשלה ומיוצג על ידו, **אינה אומרת כי אינו עצמאי בפועל.** בישראל קיימות רשויות (כגון רשם הפטנטים) שנקבע מפורשות כי הן עצמאיות, אולם הן מיוצגות על ידי היועץ המשפטי לממשלה. הדעת נותנת שהיועץ המשפטי לממשלה לא יתערב בקלות בהחלטה של גוף משפטי שמפעיל שיקול דעת מקצועי.

<u>5.1.8 – תובענה ייצוגית</u>

בקרב חברי הצוות שררה הסכמה שיש להמליץ על הוספת חוק הגנת הפרטיות לתוספת השנייה לחוק תובענות ייצוגיות, התשס״ו-2006, וזאת לאור העובדה כי המצב הקיים בחוק תובענות ייצוגיות אינו מאפשר תביעה ייצוגית, בכל העניינים הנוגעים לחוק הגנת הפרטיות. לדוגמא - כאשר המעוול הוא המדינה או מעביד. הפגיעה בגין הפרת הוראה של פרק ב׳ היא בדרך כלל פגיעה שמטיבה אין בה תמריץ מספיק ליחיד להגיש תביעה אזרחית בגין הפרתה. מאחר שמדובר בדרך

[33] עמית אשכנזי, רבקי דב״ש, חיים קלוגמן ויהושע שופמן
[34] פקודת סדרי הדין (התייצבות היועץ המשפטי לממשלה) [נוסח חדש]

ככלל במספר נפגעים רב, מפוזר, שנזקו של כל אחד קטן, נגרם כשל אכיפה. המנגנון של תביעה ייצוגית יכול להתגבר על כשלים מסוג זה, והוכח כאפקטיבי תחומים אחרים.

5.1.9 - המלצת הצוות

מוצע להוסיף בחקיקה, על סמכויותיו הקיימות של רשם מאגרי מידע, את הסמכויות או הנושאים הבאים -

1. **עצמאות שיקול הדעת של הממונה על מאגרי המידע ובכלל זה סמכותו להתייצב בהליך משפטי שיש בו עניין ציבורי הנוגע למילוי הוראות פרק ב' לחוק;**
2. **קביעת הנחיות הנוגעות לפרק ב' לחוק;**
3. **מתן סמכות לממונה לבחון תלונות שהופנו אליו בנוגע להפרה של הוראות פרק זה ולצורך בירור התלונות רשאי הממונה להורות על ביצוע פעולות פיקוח בהתאם להוראות סעיף 10(ה1) לחוק;**
4. **מתן סמכות לממונה להוציא צו אבטחת מידע בהתאם להמלצות הצוות בעניין אבטחת מידע (פרק 7.4 לדו"ח).**

כמו כן מוצע לתקן את חוק תובענות ייצוגיות כך שהחוק הגנת הפרטיות יהיה מהחוקים שהפרתם מאפשרת הגשת תובענה ייצוגית.

6 - המועצה להגנת הפרטיות

6.1 – עיגון מעמד המועצה בחקיקה

6.1.1 – המצב הקיים

" 10א. דוח הגנה על הפרטיות
לא יאוחר מ-1 באפריל בכל שנה תגיש המועצה להגנת הפרטיות לועדת החוקה חוק ומשפט של הכנסת דין וחשבון שיכין הרשם על פעולות האכיפה והפיקוח בשנה שקדמה להגשת הדוח, בצירוף הערותיה של המועצה."

כיום המועצה להגנת הפרטיות מוזכרת רק בסעיף 10א לחוק. בחוק אין הגדרה מהם תפקידי המועצה, הרכבה או דרך מינויה. בפועל, פועלת המועצה מאוקטובר 1986, לאחר שהוקמה על ידי שר המשפטים. המועצה אישרה את תקנון המועצה בשנת 1989, ותקנון זה מסדיר את מספר חברי המועצה, משך כהונתם, תחום פעילותה וכד'.

לאחרונה, פועלת המועצה להגנת הפרטיות לעגן את סמכויותיה באופן מסודר. לשם כך הכין ד"ר בירנהק בשם המועצה, בה הוא חבר, מסמך "המועצה להגנת הפרטיות – הצעה להגדרת מטרות, תפקידים וסדרי עבודה". מסמך זה, הועבר למשרד המשפטים על ידי יו"ר המועצה, עו"ד חיים קלוגמן.

6.1.2 – דעת הרוב

בקרב חברי הצוות שררה הסכמה בנוגע לעיגון קיומה של המועצה, כמייעצת לשר המשפטים, בחקיקה ראשית. עם זאת, נתגלעה מחלוקת לגבי היקף ההסדר. לדעת מרבית חברי הצוות יש להסדיר בחקיקה את סמכויות המועצה, הרכבה, דרכי מינויה וסדרי עבודתה כך שקיום המועצה לא יהיה תלוי ברצונו של משרד המשפטים ובמסירותם של חברי המועצה.

6.1.3 – דעת מיעוט[35]

לנוכח התפקיד המייעץ של המועצה, אין יתרון בעיגון חקיקתי-פורמאלי של המועצה. לדעת מיעוט חברי הצוות יתרונה של המועצה הוא בכך שהיא פועלת כגוף מייעץ באופן וולונטרי והחברים בה מקדישים את זמנם לפעילות הציבורית על בסיס המומחיות המקצועית שלהם.

6.1.4 - המלצת הצוות

מומלץ לעגן בחקיקה את תפקידי המועצה, אופן מינויה והרכבה.

[35] עמית אשכנזי, יוספה טפיירו ויהושע שופמן

7 - חובות הנלוות לניהול מאגר מידע

מאגרי המידע מהווים כיום כלי חיוני בניהול פעילות עסקית כמו גם ציבורית. מאגרי המידע מקנים יתרון לבעליהם בניהול ענייניהם ועשויים לתרום לרווחה ויעילות כלכלית. עם זאת, קיומם של מאגרי המידע עלול להוות איום על הזכות לפרטיות בשל המידע הנאגר בהם, הנגישות והיכולת לדלות ולהצליב מידע ממקורות שונים בקלות יחסית. משום כך ההסדר הקיים כיום בחוק, מבקש לאזן בין האינטרסים השונים כך שניתן יהיה להשתמש במאגרי מידע בכפוף לשמירת זכויותיהם של מושאי המידע. ההסדר הקיים בחר לעשות זאת בדרך של חובת רישום, הטלת חובות על בעלי מאגרי המידע, והענקת זכויות למושאי המידע. בהסדר זה נתגלו קשיים ביישום, ולפיכך אנו מציעים לחדד ולשפר את האיזון על ידי צמצום חובת הרישום ומנגד חיזוק עצמאות הרשם והגברת הכלים העומדים לרשותו לאכיפת החוק. בנוסף מוצע להבהיר את ההסדרים הנוגעים להטלת החובות על בעלי המאגרים והרחבת זכויותיהם של מושאי המידע.

ניהול מאגר מידע מטיל על בעל המאגר, מנהלו או מחזיקו חובות שונות שהבסיסית מביניהן היא החובה להגן על המידע המצוי ברשותו ולאבטח אותו. בעניין זה, הצוות בחן מהן החובות המוטלות על מי ששולט במאגר, בצורה זו או אחרת.

7.1 - חובות מקדמיות על בעל המאגר ומחזיקו

7.1.1 - המצב הקיים

" 8(א) לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:
(1) המאגר נרשם בפנקס;
(2) הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב1);
(3) המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

8(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

. . .

10 (א) הוגשה בקשה לרישום מאגר מידע -

(1) ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין; "

בחוק הקיים ישנם מספר תנאים מקדמיים ספורים החלים על בעל מאגר המידע –

1. חובת רישום;
2. חובה שלא לסטות מהמטרה לשמה הוקם המאגר;
3. איסור כי המאגר ישמש לפעולות בלתי חוקיות או כמסווה להן;
4. איסור לכלול מידע שנתקבל, נצבר או נאסף בניגוד להוראות כל דין.

מלבד תנאים אלו, אין תנאים מקדמיים נוספים על מי שמעוניין להקים ולנהל מאגר מידע. באיחוד האירופי, לדוגמא, יש חובות מקדמיות נוספות ועל כן הצוות בחן האם ראוי להטיל חובות נוספים על בעל המאגר.

7.1.2 - משפט משווה

7.1.2.1 – קנדה

חוק הפרטיות הקנדי מטיל על הרשויות הציבוריות שתי חובות מקדמיות –

1. אסור למוסד ממשלתי לאסוף מידע אישי אלא אם יש לו קשר ישיר לביצוע תוכנית או פעולה של אותו מוסד (סעיף 4 לחוק הפרטיות);
2. ככלל, מוסד ממשלתי יאסוף מידע ישירות ממושא המידע למעט –

א. אם מושא המידע הורה אחרת (סעיף 5(1) לחוק הפרטיות);

ב. אם ניתן לגלות לאותו מוסד את המידע המבוקש בהתאם להוראות סעיף 8(2) לחוק הפרטיות (סעיף 5(1) לחוק הפרטיות);

ג. אם איסוף מידע ישירות ממושא המידע יוביל למסירת מידע לא מדויק (סעיף 5(3) לחוק הפרטיות);

ד. אם הדבר עלול להכשיל את המטרה לשמה המידע נאסף (סעיף 5(3) לחוק הפרטיות).

לפי ההסדר ב-PIPEDA, החובה היחידה על בעל מאגר המידע, כפי שמנוסחת בסעיף 5(3) לחוק היא –

> "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

בנוסף, כל הארגונים צריכים לפעול בהתאם להוראות הקבועות בנספח הראשון לחוק (סעיף 5(1) ל-PIPEDA)[36].

הנספח כולל, בין היתר, את הדברים הבאים -

1. הטלת אחריות על הארגון לעניין המידע האישי המצוי ברשותו (סעיף 4.1 לנספח);
2. זיהוי המטרות לשמן נאסף המידע על ידי הארגון וזאת בטרם הוא מתחיל לאסוף את המידע (סעיף 4.2 לנספח);
3. היתר לעבד מידע הנדרש למטרות הארגון בלבד, בתנאי שהמידע נאסף באמצעים הוגנים וחוקיים (סעיף 4.4 לנספח).

7.1.2.2 – האיחוד האירופי

בסעיף 6 לדירקטיבה ישנן חובות כלליות המוטלות על אופן ניהול מאגר מידע כגון, חובה לעבד את המידע באופן הוגן וחוקי (fairly and lawfully) (סעיף 6(a) לדירקטיבה), איסוף מידע למטרות

[36] במקום בו הניסוח משתמש במילה "should" מדובר על המלצה ולא חובה (סעיף 5(2))

לגיטימיות ועיבוד המידע רק לאותן מטרות (סעיף 6(b) לדירקטיבה), שמירה על מידע מדויק ובמידת הצורך - מעודכן (סעיף 6(d) לדירקטיבה) וכדי .

כמו כן, סעיף 7 לדירקטיבה מונה תנאים מקדמיים, חילופיים, אשר בלעדיהם עיבוד מידע אינו לגיטימי. תנאים אלו כוללים, בין היתר, הסכמה של מושא המידע לעיבוד (סעיף 7(a) לדירקטיבה); קיומו של עיבוד מידע אם הוא נדרש לצורך ביצוע חוזה (סעיף 7(b) לדירקטיבה); קיומו של עיבוד מידע אם הוא נדרש לביצוע משימה שיש לה אינטרס ציבורי (סעיף 7(e) לדירקטיבה) ועוד.

7.1.2.3 – אירלנד

באירלנד החובות הכלליות המוטלות על אופן ניהול המאגר מצויים בסעיף 2, והתנאים המקדמיים הנדרשים על ידי הדירקטיבה מצויים בסעיף A2 לחוק האירי. ככלל, אירלנד מיישמת בחקיקה המדינתית את דרישות הדירקטיבה בשינויים קלים.

<u>7.1.3 – דעת הרוב</u>

מרבית חברי הצוות סבורים כי אין להטיל על בעליו של מאגר מידע חובות מקדמיות נוספות על החובות הקיימות כגון החובה לפעול בהתאם למטרה שהוגדרה למאגר המידע וחובת ההודעה. לשיטתם של חברי הצוות פרק ב' לחוק הגנת הפרטיות נועד להסדיר את הפעילות בתחום ההגנה על המידע והנורמות על פיהן בעל המאגר מחויב לפעול, וזאת על מנת להגן על הפרטים אודותם מצוי המידע במאגר מפני שימוש במידע ללא הסכמתם וידיעתם. קביעת חובות מקדמיות נוספות על בעל המאגר, שאינן תורמות למטרת יצירת הסדר משפטי בתחום מאגרי מידע, עלולות להוביל להתערבות שאינה נדרשת באוטונומיה של הפרט בניהול ענייניו.

<u>7.1.4 - דעת מיעוט</u>[37]

לדעת מיעוט חברי הצוות יש לקבוע הוראה בחוק האוסרת על בעל מאגר לאסוף או לשמור מידע אישי במאגר מידע מעבר לנדרש, באופן סביר, לצורך מימוש המטרה לשמה הוקם המאגר. כמו כן מוצע לציין כי איסוף מידע ושמירתו יכול להתבצע רק למטרות לגיטימיות. הפרת הוראה זו תהווה עוולה בלבד ולא עבירה פלילית.

לשיטתם, צמצום חובת רישום מאגרי המידע מחייב כי ייקבעו הוראות מהותיות נוספות אשר יקבעו את האופן בו ישמר וינוהל מאגר מידע באופן יותר דווקני[38].

<u>7.1.5 – המלצת הצוות</u>

אין צורך בתיקון חקיקה

37 עמית אשכנזי, מיכאל בירנהק, רבקי דב"ש, עומר טנא, בובי פיינדריך ואבנר פינצ'וק

38 נעיר כי לשיטתו של אבנר פינצ'וק בכל הנוגע לגוף ציבורי יש אף לאסור הקמת מאגר מידע על ידו אלא אם הדבר הכרחי למילוי תפקידו ולאחר עיגון הקמת המאגר בחקיקה.

7.2 - מתן הודעה על איסוף מידע

בעניין מתן הודעה על ידי אוסף המידע בחן הצוות אם יש להרחיב את החובה ליידע את מושא המידע על מידע שנאסף אודותיו גם באופן עקיף, ואת תוכן ההודעה המועברת למושא המידע. איסוף מידע באופן עקיף, לצורך הדיון, הינו איסוף מידע שלא ישירות ממושא המידע, בין אם על ידי איסוף ממקורות גלויים ובין אם באמצעות התחקות אחר פעולותיו של מושא.

נציין כי החשיבות במתן הודעה למושא המידע אף קיבלה הכרה במסמכים בינלאומיים בדבר הגנת מידע, והיא מגלמת את ההבנה העקרונית שעל מנת לקבל החלטה מושכלת, מושא המידע צריך להיות מודע להשלכות החלטתו. מאותה סיבה הצעת חוק הגנת הפרטיות מבקשת להוסיף להגדרת "הסכמה" בסעיף 3 לחוק כי הסכמה כאמור צריכה להיות "מדעת".

7.2.1 - המצב הקיים

סעיף 11 לחוק הקיים קובע כי -

> " 11. פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה -
>
> (1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו ;
>
> (2) המטרה אשר לשמה מבוקש המידע ;
>
> (3) למי יימסר המידע ומטרות המסירה."

החובה המוטלת על אוסף המידע למסור הודעה כאמור נועדה לממש את יכולתו של אדם להגן על פרטיותו ולאפשר לו לקבל החלטה מושכלת יותר בעת הסכמתו למסירת המידע והשימוש בו.

7.2.2 - משפט משווה

7.2.2.1 – קנדה

בקנדה, הסדר הדומה לחובת מתן הודעה קיים רק בחוק הפרטיות ולא ב-PIPEDA. החוק קובע כי –

> "5(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected."

ישנם שני חריגים לכלל זה: במקרה בו מתן ההודעה על תכלית איסוף המידע יביא לכך שהמידע שיימסר לא יהיה מדויק או כאשר מסירת הודעה כאמור תסכל את המטרה לשמה נאסף המידע (סעיף 5(3) לחוק הפרטיות).

7.2.2.2 – האיחוד האירופי

סעיף 10 לדירקטיבה קובע כי בעל מאגר מידע צריך למסור למושא המידע ממי נאסף מידע אודותיו בצירוף הפרטים הבאים:

1. זהותו של בעל המאגר ונציגו, ככל שישנו (סעיף 10(a) לדירקטיבה);

2. מטרות עיבוד המידע בשבילו נדרש המידע (סעיף 10(b) לדירקטיבה);

3. כל מידע נוסף כגון – קטגוריות המידע הנדרש, האם יש חובה למסור את המידע, למי נמסר או יימסר בעתיד המידע וכד' (סעיף 10(c) לדירקטיבה);

סעיף 11 לדירקטיבה מסדיר חובת מתן הודעה, הדומה בתוכנה להודעה לפי סעיף 10, במקום בו נאסף מידע שלא ממושא המידע. חובת ההודעה צריכה להגיע למושא המידע לא יאוחר מהמועד בו המידע נמסר או נחשף בפני צד שלישי.

7.2.2.3 – אירלנד

לפי החוק באירלנד, לא יראו עיבוד מידע כעיבוד הוגן (fairly) אלא אם יימסרו למושא המידע ממנו נאסף המידע את הפרטים הבאים (D2(2 לחוק הגנת המידע) –

1. זהותו של מחזיק המידע;
2. זהותו של נציג, ככל שמונה, למילוי הוראות חוק הגנת המידע;
3. המטרה או המטרות לשמן מבצעים עיבוד במידע;
4. כל מידע נוסף הנדרש בהתאם לנסיבות ונדרש לשם קיומו של עיבוד מידע הוגן.

מקום בו המידע נאסף ממקורות אחרים זולת מושא המידע, יש להוסיף להודעה המועברת למושא המידע, <u>עוד בטרם מתבצע עיבוד המידע</u> או בטרם המידע נמסר לצד ג', גם מידע אודות קטגוריות המידע ושמו של מחזיק המאגר המקורי ממנו נתקבל המידע (סעיף D2(3) לחוק הגנת המידע).

מכאן כי ההסדר האירי שונה מההסדר האירופי בתוכן ההודעה הניתנת למושא המידע במקום בו המידע נתקבל מאחר, וכן בחובה להעביר את ההודעה למושא המידע אף בטרם מתבצע עיבוד מידע אודותיו.

<u>7.2.3 – מרבית חברי הצוות</u>[39]

חברי הצוות סבורים כי אין להטיל חובת יידוע בגין איסוף מידע באופן עקיף.

הטעם לכך הוא שמדובר בהטלת נטל בלתי סביר על אוסף המידע, לדוגמא כאשר איסוף המידע נעשה ממקורות גלויים.

לדעת הצוות ככל שיש באיסוף המידע או באופן בו נעשה שימוש במידע פגיעה אסורה בפרטיות, חלות הוראות סעיף 2 לחוק האוסר על איסוף או שימוש כאמור. לשיטתם, יש להבחין בין ההגבלות הקיימות על איסוף המידע עצמו לבין הטלת חובה, פרוצדוראלית במהותה אם כי נועדה להבטיח זכות מהותית, למסור הודעה על איסוף המידע. מילוי אחר הוראות סעיף 11 כלשונן אין בו כדי להכשיר איסוף מידע אסור - לדוגמא, לפי סעיף 2 לחוק הגנת הפרטיות. בנוסף, מובן שזכות העיון וזכות התיקון עדין עומדת לרשות מושא המידע, גם אם המידע אודותיו נאסף מצד שלישי.

---

[39] למעט דלית דרור

עם זאת הוצע להרחיב את פרטי ההודעה מעבר למה שהחוק מחייב כיום. מוצע כי מעבר לפרטים הנדרשים כיום, יש להודיע לאדם ממנו נאסף המידע על מקור החובה החוקית לאיסוף המידע, במידה שישנה חובה כזו, פרטים על זכויותיו ביחס למידע ופרטי דרכי ההתקשרות עם מבקש המידע[40].

<u>7.2.4 - המלצת הצוות</u>

מוצע לתקן את סעיף 11 כך שבחובת ההודעה יכללו גם הפרטים הבאים:

1. **מקור החובה החוקית לאיסוף המידע, במידה שישנה חובה כזו;**
2. **פרטים על זכויות מושא המידע ביחס למידע שנאסף ממנו;**
3. **פרטים על דרכי ההתקשרות עם מבקש המידע.**

[40] ההמלצה היא להתאים את פרטי ההודעה כפי שהוצע בתזכיר החוק לפני שהוחלט על השמטת התיקונים הנוגעים לפרק ב'.

7.3 – העברת מידע ממאגר המידע

אגב הדיון בשימוש במידע המצוי במאגר, עלתה השאלה האם יש לקבוע הוראה מיוחדת לגבי העברת מידע ממאגר המידע מבלי להתייחס לתוכנו של המידע. סעיף 2(9) אוסר על העברת ידיעות על ענייניו הפרטיים של אדם שלא למטרה שלשמה נמסרו. עם זאת, אין מניעה להתיר העברת מידע רב ממאגר מידע ככל שהמידע אינו נוגע ל"ענייניו הפרטיים של אדם". לפיכך הצוות נדרש לשאלה האם העברת מידע גורפת, גם אם אינה נוגעת ל"ענייניו הפרטיים של אדם", דורשת הסדרה כך שלא תתאפשר העברת המידע למאגר אחר שלא למטרה שלשמה נדרשה.

7.3.1 – דעת הרוב

לדעת מרבית חברי הצוות, בשל כמות המידע הנצברת במאגר מידע והאפשרות לערוך עליו מניפולציות מיחשוביות, יש להוסיף הוראה האוסרת על העברת ידיעות גם אם אינן בגדר "ענייניו הפרטיים של אדם", וזאת כאשר העברת המידע אינה של פריטי מידע בודדים, אלא של חתך רחב הנגזר ממאגר המידע. לאור ההתקדמות בתחום כריית המידע, קיים חשש מפני העברת חתכים ממאגרי מידע, גם אם העברת המידע אינה אסורה לפי סעיף 2(9) לחוק, וזאת לאור האפשרות להצליבם עם מאגרי מידע נוספים. לפיכך מרבית חברי הצוות סבורים שיש לאסור על העברת כל מידע אישי ממאגרי מידע. נדגיש כי אין באמור כדי לפגוע בהעברת מידע ממאגרים הפתוחים לעיון הציבור או במקום בו ניתנה הסכמתם של מושאי המידע להעברת המידע.

7.3.2 – דעת המיעוט[41]

לדעת מיעוט חברי הצוות אין צורך בסעיף כמוצע על דעת רוב חברי הצוות. בתי המשפט נוהגים לפרש את סעיף 2(9) לחוק ולהחיל אותו על פריטי המידע הטרוויאלים ביותר. לכן, העברת מידע ממאגר למאגר בלא הרשאה ממושא המידע תבוא בהכרח בגדר סעיף 2(9). לא זאת בלבד, אלא שהתיקון המוצע גורם לחוסר בהירות בדבר פעולתו האמיתית של סעיף 11: סעיף 11 מחייב מתן הודעה מפני שהוא מניח שמי שקיבל הודעה ומסר את פרטיו – ביטא בכך את הסכמתו. אם ניתנה הודעה לפי סעיף 11 בדבר העברת מידע – אין מקום לאסור על העברת מידע ממאגר המידע. אם לא ניתנה הודעה כזו – העברת המידע מהווה לכאורה הפרה של התחייבות כלפי מושא המידע.

7.3.2 – המלצת הצוות

מוצע לאסור העברת חתך רחב של מידע אישי לגורם אחר, אלא למטרה לשמה נמסר המידע, למעט אם המידע הועמד לעיון הציבור או נתקבלה הסכמתם של מושאי המידע.

[41] עומר טנא וחיים רביה

7.4 - אבטחת מידע

7.4.1 - המצב הקיים

לפי הדין בישראל, כל אחד מאלה אחראי על אבטחת המידע – בעל המאגר, המחזיק והמנהל (סעיף 17 לחוק).

מי שמחזיק ביותר מחמישה מאגרי מידע השייכים לבעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשה לכך במפורש בהסכם בכתב בינו לבין בעלי אותו מאגר (סעיף 17א(א) לחוק). במידה שמאגרי המידע המצויים בידי מחזיק כאמור הם מאגרים החייבים ברישום, צריך המחזיק להוסיף תצהיר לרישום המאגרים על כך שלגבי כל אחד מהמאגרים קיים הסכם בכתב המגדיר את בעלי הגישה לכל מאגר (סעיף 17א(ב) לחוק).

בישראל קיימת חובה למנות אדם בעל הכשרה מתאימה שיהיה אחראי על אבטחת המידע במקרים הבאים, וזאת מבלי לגרוע מאחריותם של בעלי התפקידים לפי סעיף 17 לחוק:

1. המחזיק בחמישה מאגרים החייבים ברישום (סעיף 17ב(א)(1) לחוק);
2. גוף ציבורי כהגדרתו בחוק (סעיף 17ב(א)(2) לחוק);
3. בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי (סעיף 17ב(א)(3) לחוק).

7.4.2 - משפט משווה

7.4.2.1 – קנדה

בחוק הפרטיות הקנדי אין התייחסות לאבטחת המידע המצוי בידי הרשויות[42].

ה-PIPEDA קובע את הסטנדרטים לאבטחת מידע בסעיף 4.7 לנספח לחוק, המפרט את כל חובות בעלי מאגר המידע בנושא זה. הכלל הוא כי מידע אישי צריך להיות מוגן באמצעי אבטחה התואמים את רגישות המידע (סעיף 4.7 בנספח ל-PIPEDA). פירוט חובות אבטחת המידע כולל המלצה[43] כי אבטחת המידע תכלול התייחסות לגורמי האבטחה הבאים: הגנה פיזית על מאגר המידע, מדדים ארגוניים כגון הרשאות גישה על בסיס צרכי העבודה ואמצעים טכנולוגיים (סעיף 4.7.3 בנספח ל-PIPEDA).

7.4.2.2 - האיחוד האירופי

סעיף 17 לדירקטיבה האירופית עוסק בתחום אבטחת המידע. החובה של מדינות האיחוד היא להורות לבעל מאגר המידע להשתמש באמצעים טכנולוגיים וארגוניים על מנת להבטיח את ההגנה על המידע האישי. אמצעים אלו צריכים להיות מותאמים לסיכונים הנובעים מעיבוד המידע ורגישות המידע המצוי במאגר (סעיף 17(1) לדירקטיבה). בבחירת גורם מקצועי המבצע עבור בעל המאגר את עיבוד המידע, חייב בעל המאגר לדאוג כי לאותו גורם יש אמצעים מתאימים לאבטחת המידע (סעיף 17(2) לדירקטיבה) ונושא זה צריך להיות מוגדר בחוזה כתוב[44] או בחובה משפטית מחייבת בין בעל המאגר למי שפועל מטעמו (סעיף 17(3) לדירקטיבה).

---

[42] עם זאת החוק קובע סעיפי סודיות מפורטים וקפדניים כאשר הכלל הוא כי מוסד ציבורי לא יעשה שימוש במידע אישי המצוי ברשותו ללא הסכמת מושא המידע אלא למטרה לשמה נשמר המידע או במקרים המפורטים בסעיף 8(2) לאותו חוק (סעיף 7 לחוק הפרטיות).

[43] הסעיף משתמש במינוח "should", המהווה המלצה ולא חיוב לבעל המאגר.

[44] חובת הכתב מופיעה בסעיף 17(4) לדירקטיבה.

7.4.2.3 – אירלנד

סעיף 2(1)(d) לחוק באירלנד מטיל חובה על בעל המאגר לנקוט בצעדים המבטיחים את ההגנה על המידע. הסעיף מנוסח בדומה לסעיף 17(1) לדירקטיבה אולם באופן עמום יותר. לדוגמא, אחד ההבדלים בין הנוסחים הוא שהחוק באירלנד משתמש במושג "appropriate security measures" ולא במינוח "appropriate technical and organizational measures" בו נעשה שימוש בדירקטיבה.

עם זאת, סעיף C2 לחוק הגנת המידע מפרט מה הם הפרמטרים אליהם יתייחס בעל מאגר על מנת לפעול בהתאם לסעיף 2(1)(d) באותו חוק. בין היתר ישנה התייחסות לנזק העלול להיגרם מחשיפת מידע שלא כדין ורגישותו של המידע המצוי במאגר (סעיפים C2(1)(b)(i) ו-C2(1)(b)(ii) לחוק הגנת המידע - בהתאמה). נוסף לחובות המצוינות בדירקטיבה, מחייב החוק באירלנד את בעל המאגר לנקוט באמצעים סבירים על מנת שעובדיו ובני אדם אחרים המצויים במקום העבודה, שהנושא עלול להיות רלוונטי עבורם, יהיו מודעים לאמצעי אבטחת המידע הרלוונטים ויפעלו לפיהם (סעיף C2(2) לחוק הגנת המידע).

7.4.3 – הסכמה כללית

בנושא אבטחת המידע שררה בצוות הסכמה כללית לגבי שתיים מתוך שלוש ההמלצות בנושא זה:

1. סטנדרט אבטחת המידע לא יהיה תלוי בתקינה[45];
2. יש לצמצם את אי-הוודאות של בעלי המאגרים ומחזיקי המאגרים ובו בזמן ליתן בידי הרשם סמכות אכיפה, בדרך של "תקינה אישית";
3. יש לנסות להגדיר בצורה ברורה חובה של בעל מאגר להודיע על פגיעה בפרטיות, ברוח ההסדר הקיים בקליפורניה, כמפורט בסעיף 7.4.3.3.

7.4.3.1 – סטנדרט אבטחת המידע

לדעת הצוות אין לתלות את אבטחת המידע המחויבת מכוח החוק בתקינה של סטנדרטים לאבטחת מידע. הטעם לכך הוא שהאופן בו בעל מאגר מידע מממש את חובתו להגן על המידע המצוי בידו, משתנה בהתאם לאיומים על המאגר ולמערכות האבטחה החדשות הקיימות בשוק – שני מושגים המשתנים חדשות לבקרים. בניגוד לשינויים המהירים בשוק זה, הליכי התקינה אורכים זמן רב כך שהשוק, לעתים, מוצא פתרונות לאבטחת מידע שהם בטוחים יותר מפתרון שקיבל אישור של מכון תקינה רשמי. מכיוון שהתקינה אינה דינאמית דיה כדי להתאים עצמה לשיפור הטכנולוגיה ולאיומים עליה, אין לקבוע שאמת המידה לאבטחת המידע הנדרשת בחוק תיקבע בתקינה[46]. מנגד, בעלי מאגרי המידע ומחזיקיהם מבקשים הנחייה ברורה משפטית יותר אלא, שבגלל הקושי האמור, אין מנוס אלא לבחור בדרך של סטנדרט, להבדיל מכלל פרטני.

---

[45] למעט עמית אשכנזי

[46] נציין כי היה מי שסבר בצוות שהקושי בתקינה הקיימת היא שהתקינה מוכוונת לארגונים המבקשים להתמודד עם סיכוני אבטחת מידע כמטרה מרכזית וככאלה הם עלולים להציב רף גבוה מדי לארגונים אחרים.

עם זאת, מוצע לתקן את סעיף 17 כך שיובהר מהי הנורמה הראויה לאבטחת מידע. לפיכך מוצע להוסיף לחוק את דרישת הסבירות. כוונת הצוות היא להדגיש בחוק כי חובתם של הגורמים האחראים לכך להתקין אמצעי הגנה במאגר המידע התואמים לרגישות המידע השמור במאגר המידע ולאופן בו המידע נשמר.

מוצע כי הנוסח החדש יציג את הרף האובייקטיבי שישמש לפרשנות בתי המשפט ביחס לחובות בעל המאגר במסגרת עוולת הרשלנות, וישתמש במונחים המקובלים בקרב מומחי אבטחת מידע - שלמות (integrity), זמינות (availability), סודיות (confidentiality) ושימוש לא מורשה (unauthorized access) – תוך ניסיון ליצור אחידות מסוימת עם האיסורים הקבועים בחוק המחשבים, התשנ"ה-1995[47].

7.4.3.2 – תקינה אישית

כדי לקבוע רף מינימאלי להגנה במקרים מיוחדים ומתאימים, מציע הצוות לקבוע הסדר על פיו ניתן להוציא, לגבי מאגר מסוים שאינו מאובטח כראוי, צו אבטחת מידע. הרשם, או עובד ציבור שהוא הסמיך לכך, יוסמך להורות למי שחייב באבטחת מידע לנקוט פעולות הנוגעות לאבטחת המידע, כפי שיפורט בצו. אי קיום הצו יוביל להטלת קנס על האחראי לאבטחת המידע.

מתן סמכות כאמור לרשם מאגרי המידע או לעובד מדינה מטעמו, יאפשר ליחידת הרשם להתאים הוראות אבטחת מידע בהתייחס למאגר ספציפי, תוך מתן הכלים להרתיע מי שלא יפעל בהתאם לצו.

הסדר דומה נקבע לאחרונה בחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998[48], המסמיך את נציב שוויון זכויות אנשים עם מוגבלות להוציא "צו נגישות" למקום שאינו נגיש לאדם עם מוגבלות.

7.4.3.3 – חובת בעל מאגר ליידע על כשל באבטחת המידע

מדינת קליפורניה יצרה הסדר המחייב בעלי מאגר להודיע למושאי המידע על כשל באבטחת המידע שבעקבותיו דלף מידע אישי שאינו מוצפן, או כאשר ישנו חשש שנלקח מידע מסוג זה[49] (סעיפים 1798.29 ו-1798.82-1798.84 לקוד האזרחי בקליפורניה).

ההסדר מחייב כל בעל מאגר מידע לגבי מידע אישי אודות תושב קליפורניה. מידע אישי, לפי הוראות החוק הוא מידע הכולל את שמו של אדם בצירוף אחד הפרטים הבאים: מספר הביטוח הלאומי (social security number), מספר רישיון הנהג או מספר תעודת הזהות הקליפורנית, מספר חשבון בנק או כרטיס אשראי בצירוף סיסמה אשר מאפשרת גישה לחשבונות הפרט.

עמדת הצוות היא, כי יש לחייב בעל מאגר מידע במתן הודעה למי שמידע אישי אודותיו דלף, או, במידה שמדובר במידע אישי אודות מספר גדול של בני אדם, בפרסום הודעה לציבור. ההצעה תאפשר למושאי המידע לדעת מה עלה בגורל המידע אודותיהם, ולכלכל את צעדיהם הצרכניים והמשפטיים בהתאם. בנוסף, הסדר כאמור יכול להיות תמריץ לבעלי מאגרי מידע לנקוט אמצעי אבטחת מידע סבירים, כנדרש בחוק. עם זאת, יש צורך כי ההסדר ינוסח באופן בהיר כך שהחובה

---

[47] ס"ח התשנ"ה, עמ' 366.

[48] ס"ח התשנ"ח, עמ' 152; הסדרת צו הנגישות פורסם בס"ח התשס"ה, עמ' 288.

[49] שימוש בתום לב על ידי עובד הארגון בו מצוי המאגר, שלא בהתאם להוראות אבטחת המידע, כאשר לא נעשה שימוש לרעה נוסף במידע, אינו מחייב מתן הודעה.

תהיה ברורה וימנע המצב בו ההוראה תהפוך לאות מתה. ההסדר המוצע, בשילוב עם הצעת הצוות לאפשר תביעות ייצוגיות בגין הפרת חוק הגנת הפרטיות, תאפשר אכיפה פרטית אפקטיבית נגד מפירי הוראות החוק.

<u>7.4.4 - המלצת הצוות</u>

7.4.4.1 – סטנדרט אבטחת המידע

מוצע להחליף את סעיף 17 הקיים בסעיף המוצע –

(א) בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע;

(ב) אמצעי אבטחת המידע יבטיחו הגנה סבירה על שלמות המידע, זמינותו*, וסודיותו* וימנעו שימוש בלתי מורשה* בו, לרבות עיון, העתקה או שינוי של המידע.

* הערה: על המחוקק להגדיר מושגים אלו

7.4.4.2 – תקינה אישית

מוצע לתת סמכות לרשם מאגרי המידע לתת צווים אישיים בדומה להסדר הקיים בסעיף 19מג לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998.

7.4.3.3 – חובת בעל מאגר ליידע על כשל באבטחת המידע

מוצע לאמץ בחקיקה הסדר דומה במהותו להסדר הקליפורני, בשינויים המחויבים.

7.5 – אבטחת מידע במאגרי מידע ממשלתיים

7.5.1 - מאגרי מידע ממשלתיים

השאלה שהתעוררה בקרב חברי הצוות, אגב הדיון באבטחת המידע, היא האם יש להבחין בין החובה המוטלת על מאגרי מידע ממשלתיים לבין החובה המוטלת על מאגרי מידע פרטיים.

7.5.2 - דעת הרוב

לדעת מרבית חברי הצוות אין ליצור בחוק הגנת הפרטיות הבחנה בין חובת האבטחה במאגרי מידע ממשלתיים לבין חובה זו במאגרי מידע פרטיים. הטעם לכך הוא כי חובת אבטחת המידע נגזרת מסוג המידע המצוי בידי בעל המאגר ואופן אחזקתו ולא מאפיונו של בעל המאגר. עמדה זו אף קיבלה חיזוק בהמלצת הצוות בסעיף 7.4.4.1 לעיל, המציעה כי חובתם של הגורמים האחראים לכך להתקין אמצעי הגנה במאגר המידע יותאמו לרגישות המידע השמור במאגר המידע ולאופן בו המידע נשמר.

החשש מפני המידע הרב המצוי במאגר מידע והיכולת לעשות בו שימוש ללא שליטתו של מושא המידע קיים גם כאשר המידע מצוי בידיים פרטיות. להפך, לעתים העדר ביקורת בשוק הפרטי עלולה להוביל ליכולת רבה יותר לפגוע בפרטיות מבלי שהציבור ידע על כך. נדגיש כי המדינה והרשויות שבידיהן מאגרי מידע כפופות, נוסף על חוק הגנת הפרטיות, לעקרונות של המשפט המנהלי והחוקתי, כפי שנקבעו בפסיקה, כמו למשל עקרונות הסבירות והמידתיות.

7.5.3 - דעת מיעוט[50]

לדעת מיעוט חברי הצוות יש להטיל חובה מוגברת על מאגרי מידע ממשלתיים. היקף המידע במאגרי מידע ממשלתיים, מהימנותו ועדכניותו גבוהים על-פי רוב לאין ערוך מאלה של מאגרי מידע פרטיים. בין השאר, מאגרים אלה שואבים את נתוניהם ממידע שחייב אדם למסור לפי דין – או שאחר חייב למסור אודותיו (לדוגמה: נתוני המעביד על שכרו של עובד יימסרו לביטוח הלאומי ולמס הכנסה; נתונים בדבר מצבו הרפואי של פלוני ייאגרו מתוקף שירותו הצבאי וכיו"ב). ניסיון העבר מלמד שממאגרים ממשלתיים נשקף סיכון גבוה לפרטיותם של יחידים. מאגרים אלה שימשו בין השאר מקור למידע שדלף ואף נמכר לשוק הפרטי. בהתחשב בסכנה מוגברת זו, מחד גיסא, ומהיקף המשאבים שבידי השלטון, מאידך גיסא, ראוי שהממשלה תחויב לאבטח את המידע ולקבוע נהלי גישה מחמירים אליו, במידה רבה יותר מאשר הסקטור הפרטי.

נקודת המוצא להבחנה היא שמידע שנאגר בידי המדינה נאסף בדרך כלל באופן לא רצוני, והוא חלק מהחיים במדינת רווחה מודרנית. יש רבגוניות בשיטות איסוף המידע וביזור בשימוש בו. עולה חשש שמי שמופקד על שמירת המידע אינו תמיד "מפנים" את הסיכון הכרוך באותו מידע. חשש דומה עולה גם כאשר נעשה שימוש במשאבים חומריים בממשלה, אולם לצורך כך נקבעו בקרות נוהליות והפרדות נוהליות (חתימה של חשב, אישור יועץ משפטי, בקרה תקציבית). מערכות בקרה אלה אינן קיימות כאשר המדובר במידע.

על מנת לוודא כי המדינה על שלל זרועותיה עומדת בהוראות החוק, יש צורך במנגנוני פיקוח מוגברים.

---

[50] עמית אשכנזי וחיים רביה

חשש נוסף קשור במציאות של מדינת המינהל המודרנית, הפועלת באמצעות ספקים חיצונים וקבלני משנה. בנקודה זו יש לוודא כי כאשר מבוצעים תפקידים באמצעות גורמים שלישים, שלכאורה אינם כפופים לאותן חובות כמו הרשות (אלא על פי כישרונם של נסחי החוזים עם אותם גורמים שלישים) יעשו בקרות פנימיות. בנושא מחשוב, ייתכן שחברה פרטית גדולה אחת מחזיקה מאגרים של מספר משרדים ממשלתיים. כל אחד מהם כשלעצמו עומד בהוראות החוק, אולם אותם משרדים אינם מודעים לכך שחברה פרטית מחזיקה את מלוא המידע שיש לכל אחד מהם בנפרד.

<u>7.5.4 - המלצת הצוות</u>

אין צורך בתיקון חקיקה.

7.6 – סודיות

7.6.1 - המצב הקיים

> " 16. לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי; אם הוגשה הבקשה לפני תחילת ההליך תידון הבקשה בבית משפט השלום.
> המפר הוראות סעיף זה, דינו - מאסר 5 שנים "

סעיף סודיות זה חל על הגופים הציבוריים והפרטיים כאחד. עם זאת יש להדגיש כי חובת הסודיות החלה על גופים ציבוריים מקורה בהוראות חוק נוספות וביניהן - סעיף 23ב(א) לחוק, סעיף 117 לחוק העונשין, התשל"ז-1977, סעיפי סודיות ספציפיים דוגמת סעיף 234 לפקודת מס הכנסה ועוד.

7.6.2 - משפט משווה

בהתייחסותנו למשפט המשווה בחנו הוראות סודיות כלליות החלות גם על גופים פרטיים, ולא הוראות חוק החלות על גופים ציבוריים בלבד.

7.6.2.1 - קנדה

סעיף 5(3) ב-PIPEDA אוסר על מסירת ללא ידיעתו או הסכמתו של מושא המידע, למעט בסיטואציות מסוימות, ביניהן –

א. מסירת המידע לבא כוחו של הארגון (סעיף קטן (a));

ב. מסירת המידע לצורך גביית חוב של מושא המידע למחזיק המידע (סעיף קטן (b));

ג. מסירת המידע לפי זימון או צו של בית משפט (סעיף קטן (c));

ד. מסירת המידע התבצעה לאחר 100 שנה מהיווצרות רישום המידע אצל המחזיק או 20 שנה לאחר פטירתו של מושא המידע – לפי המאוחר מבין שניהם (סעיף קטן (h));

7.6.2.2 – האיחוד האירופי

הדירקטיבה האירופית ניסחה את חובת הסודיות באופן הבא (סעיף 16 לדירקטיבה) -

> "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."

7.6.2.3 – אירלנד

ראו האמור בפרק 7.4.2.3 לדו"ח

7.6.3 – הסכמה כללית

חברי הצוות מסכימים כי אין צורך לשנות את הנוסח הקיים למעט שני תיקונים קלים –

1. יש לשנות המינוח "לצורך ביצוע עבודתו" כך שיהיה איסור על שימוש במידע למטרה שונה מזו לשמה נאסף ונשמר המידע (עקרון צמידות המטרה);
2. הסנקציה בגין הפרת חובת הסודיות תהיה פחותה מחמש שנים. הצורך בהגברת האכיפה והענישה בנושא הגנת הפרטיות עמד לנגד עיניי הצוות. עם זאת, יש לוודא כי העונשים הנקבעים בחקיקה תואמים את חומרת המעשה, כך שלא ייווצר פער גדול מִדי בין העונש שקבע המחוקק לענישה בפועל. נעיר עוד כי הצוות סבר כי אין מקום להשוות את דינו של מי שהפר את חובת הסודיות לדינו של מי שפגע בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, ובוודאי שלא להחמיר על העונש שנקבע לגבי עובד ציבור שמסר ידיעה ללא סמכות כדין[51].

7.6.5 - המלצת הצוות

מוצע לתקן את סעיף 16 כך –

1. **שיעוגן עקרון צמידות המטרה;**
2. **שהסנקציה בגין הפרת החובה תהיה פחותה מהקבוע היום.**

[51] העונש במקרה זה עומד על שלוש שנות מאסר. סעיף 117(א) לחוק העונשין, התשל"ז-1977

8 – זכות העיון והתיקון

8.1 –זכות העיון

8.1.1 המצב הקיים

"13. (א) כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

. . .

(ג) בעל המאגר רשאי שלא למסור למבקש מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו;במקרה זה ימסור בעל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש.

(ג1)אין בהוראות סעיף זה כדי לחייב למסור מידע בניגוד לחסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחסיון נועד לטובתו."

8.1.2 - משפט משווה

8.1.2.1 – קנדה

חוק הפרטיות הקנדי מקנה לכל אזרח או תושב גישה למידע אישי המתייחס אליו, והנמצא אצל הרשויות (סעיף 12(1) לחוק הפרטיות). נציין שהוראות החוק למתן זכות עיון במאגרי המידע של הרשויות דומות להסדרים לעיון לפי חוק חופש המידע, התשנ"ח-1998 (להלן – **חוק חופש המידע**)[52] יותר מאשר להסדרים המקנים זכות עיון במידע לפי הוראות חוק הגנת הפרטיות.

ההתייחסות לזכות העיון ב-PIPEDA מצויה בחוק כמו גם בנספח לו. עיגון הזכות מצוי בסעיף 4.9 לנספח לחוק, אליו גם מפנה סעיף 8 לחוק. החוק מציין כי בקשה לעיון צריכה להימסר בכתב (סעיף 8(1) ל-PIPEDA), צריך לתת לה מענה תוך 30 יום (סעיף 8(3) ל-PIPEDA) והארגון יכול להאריך את המועד ב - 30 יום נוספים במקרים מיוחדים (סעיף 8(4) ל-PIPEDA). אי מתן מענה במועד יחשב כסירוב למסירת מידע (סעיף 8(5) ל-PIPEDA). הארגון ממנו מתבקש המידע יכול להטיל על המבקש תשלום העלות הכרוכה במסירת המידע רק אם הוא הודיע למבקש המידע על הסכום אותו הוא ידרוש ומבקש המידע לא הודיע כי הוא מושך את בקשתו (סעיף 8(6) ל-PIPEDA).

המידע שיימסר יכלול הודעה אם קיים מידע על המבקש, אם לאו, איזה שימוש נעשה במידע ולאלו צדדים שלישיים נחשף המידע. כמו כן, החוק מעודד את הארגונים למסור מידע גם אודות מקורות המידע (סעיף 4.9.1 לנספח ל-PIPEDA). המידע צריך להימסר תוך זמן סביר ובעלות מינימאלית (אם בכלל) למבקש המידע. המידע יימסר בשפה המובנת באופן כללי, דהיינו, אם הארגון עושה שימוש בקודים, יש לבאר למבקש המידע מה משמעות הקודים בהם נעשה שימוש (סעיף 4.9.4 לנספח ל-PIPEDA).

[52] ס"ח תשנ"ח, עמ' 226

8.1.2.2 – האיחוד האירופי

הדירקטיבה מורה כי מדינות האיחוד יבטיחו שמושא מידע יוכל לקבל מבעל מאגר מידע את המידע הבא (סעיף 12 לדירקטיבה):

1. פירוט אם נעשה עיבוד של המידע אודותיו, מטרת עיבוד המידע, קטגוריות המידע בהן מבוצע עיבוד של המידע ולמי מועבר המידע;
2. מסירת המידע המצוי בידיהם וככל שניתן, מקורות המידע;
3. מתן הרציונל העומד בבסיס הצורך לבצע עיבוד אוטומטי במידע אודות מושא המידע.

8.1.2.3 – אירלנד

הזכות לעיון במידע באירלנד אף היא צריכה להתבצע בכתב, ועל בעל המאגר למסור את הפרטים הבאים (סעיף 4(1)(a) לחוק הגנת המידע):

1. האם קיים מידע אודות המבקש ואם כן –
2. קטגוריות המידע בהן נעשה עיבוד מידע;
3. המידע האישי שיש אודות המבקש;
4. מקורות המידע (למעט אם מדובר במידע הפתוח לעיון הציבור);
5. המטרות לשמן עובד המידע;
6. למי מועבר המידע.

עלות הטיפול בבקשה מוטלת על מבקש המידע, אולם במידה שבקשתו לא נענתה, יש להשיב לו את הסכום אותו שילם (סעיף 4(1)(c) לחוק הגנת המידע). בחוק הגנת המידע האירי יש מספר הוראות ייחודיות כגון בהתייחס למסירת מידע אודות הבעת דעה של גורם שלישי על מושא המידע (סעיף 4(A4)(a) לחוק הגנת המידע) וכן התייחסות ספציפית למסירת מידע אודות תוצאות בחינה (סעיף 4(6)(a) לחוק הגנת המידע).

8.1.3 – מרבית חברי הצוות[53]

זכות העיון היא מרכיב חיוני ויסוד מרכזי בהסדר של ההגנה על זכויותיהם של מושאי מידע. הזכות נועדה להשיג מטרה ישירה, של שקיפות המידע שבמאגרים בפני מי שהמידע הוא אודותיהם, ובכך למנוע את החשש מהמצב הקפקאי בו קיימים מאגרים סודיים. זכות העיון נועדה לשרת את יכולת הפיקוח של מושא המידע, לוודא שבעל המאגר קיים את חובותיו שלפי סעיף 11, ואת החובה שלא לחרוג מהשימוש המותר במידע. משום כך, אנו סבורים כי יש מקום להרחיב ולבצר את הזכות, כדי ליצוק לתוכה תוכן ממשי. הרחבה זו באה יד ביד עם התיקון המוצע בתיקון מס' 9, בקשר להגדרת "הסכמה מדעת".

[53] למעט יובל אלוביץ

לפיכך, לדעת מרבית חברי הצוות יש להרחיב את זכות העיון גם לקבלת המידע הבא:

1. סוג המידע המצוי במאגר (מידע רפואי, הרגלי צריכה וכד')
2. למי נמסר המידע המצוי במאגר;
3. מהם מקורות המידע מהם מתקבל המידע השמור במאגר[54].

ההרחבה של היקף המידע שניתן על בסיס זכות העיון, נועדה לאפשר לאדם ידיעה מלאה וביקורת על אופן השימוש במידע אודותיו. לצורך כך, לא מספיקה הידיעה בדבר המידע האישי המצוי במאגר, אשר בדרך כלל מוכר למושא המידע, אלא נדרשת ידיעה נוספת בנושאים המוצעים על ידי הצוות. החשיבות בהרחבה היא גם במקרה שהמידע נאסף שלא על ידי פנייה ישירה למושא המידע, אלא באמצעות צד ג'.

__8.1.4 - המלצת הצוות__

מוצע כי החוק יתוקן כך שזכות העיון תכלול גם קבלת מידע בנושאים הבאים -

(1) סוג המידע האישי השמור במאגר המידע;

(2) מקורות המידע של מאגר המידע;

(3) האם המידע האישי השמור במאגר מועבר לצדדים שלישיים;

(4) במידה שמידע אישי מועבר לצדדים שלישיים, מי הם אותם צדדים ומהן המטרות לשמן מועבר המידע.

---

[54] נציין כי לעניין מסירת מידע אודות מקורות המידע, נחלקו חברי הצוות לגבי היקף החובה. מרבית חברי הצוות סבורים יש לחייב מסירת כלל מקורות המידע ואין צורך למסור מידע אודות המקורות הספציפיים מהם נאסף המידע אותו אדם. הטעם לכך הוא בנטל הנוסף המטילים על בעלי המאגר – שמירת המקורות הספציפיים של כל ידיעה. נוסף על כך, לאדם שמידע אודותיו נמצא במאגר מידע מחוץ לשליטתו יש עניין בכלל המקורות מהם נאסף מידע מכיוון שייתכן כי בעתיד מקורות אחרים יעבירו עליו מידע.
מיעוט חברי הצוות סבר כי בעל מאגר מידע צריך לאפשר למושא המידע לקבל מידע אודות המקורות ששימשו לאיסוף המידע אודותיו בלבד, ככל שניתן.

8.2 – עלות זכות העיון

8.2.1 - המצב הקיים

"13(ד) האופן, התנאים והתשלום למימושה של זכות העיון במידע ייקבעו בתקנות."

בתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981[55], שנקבעו מכוח סעיף 13(ד) לחוק הגנת הפרטיות, נקבע כי -

"6. המבקש לעיין במידע כאמור בתקנות אלה ישלם לבעל או למחזיק של מאגר המידע תשלום בסך 20 שקלים."

נציין כי התקנות לא עודכנו מיום שנכנסו לתוקף, למעט תיקון עקיף בנוגע לפרוצדורה בהגשת ערעור על סירוב לעיין במידע[56]. נעיר כי מדובר בשקלים ישנים כך שהתשלום המעוגן בחוק עומד על סך של 2 אגורות חדשות.

8.2.2 - משפט משווה

ראו התייחסות לעיל (פרק 8.1.2)

8.2.3 – הסכמה כללית

לדעת חברי הצוות קיים קושי בקביעת מחיר אחיד עבור זכות העיון וזאת מכיוון שההוצאות המוטלות על בעל מאגר מידע בגין הפקת המידע שבידו, נקבעות לפי סוג הטכנולוגיה בה נעשה שימוש ואופן שמירת המידע ושונות ממאגר למאגר. עם זאת עולה החשש שאם שיקול הדעת יוותר בידי בעל מאגר המידע, עלולה עלות הזכות להוות מחסום בפני מימושה.

לפיכך מוצע כי יקבע מחיר מקסימאלי עבור מימוש זכות העיון, אולם בעל מאגר מידע שירצה לגבות סכום הגבוה מהמחיר שנקבע, יצטרך לפנות לרשם בבקשה מנומקת על מנת לקבל אישור לחריגה במחיר. כמו כן מוצע כי הרשם יפרסם את דרישת בעל המאגר, יקבל הערות מהציבור ויחליט האם לקבל את הבקשה של בעל המאגר. החלטתו המנומקת של הרשם תפורסם ברבים.

8.2.4 - המלצת הצוות

מוצע לתקן את החוק כך שיפורסם סכום התשלום המקסימאלי למימוש זכות העיון, מחיר שיעודכן אחת לתקופה. בעל מאגר אשר יבקש לגבות מחיר העולה על הסכום שנקבע, יצטרך לפנות לרשם על מנת שיאשר את המחיר החריג. לאחר שהפניה של בעל המאגר תובא לידיעת הציבור, הרשם יפרסם את החלטתו המנומקת ברבים.

כמו כן הצוות ממליץ למשרד המשפטים לבחון מחדש את תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981, ולהתאים את הוראות התקנות לזמננו.

[55] פורסם בק"ת התשמ"ט, עמ' 1480
[56] פורסם בק"ת התשס"ב, עמ' 1267

8.3 – השפה בה יימסר המידע

8.3.1 - המצב הקיים

כיום החוק קובע כי -

"13(ב) בעל מאגר מידע יאפשר עיון במידע, לפי בקשת אדם כאמור בסעיף קטן (א) (להלן - המבקש), בשפה העברית, הערבית או האנגלית."

8.3.2 – הסכמה כללית

לדעת הצוות אין להטיל על בעל המאגר חובה לתרגם את המידע המצוי בידו לשפה השונה מהשפה בה שמור המידע. לעניין זה נציין כי אף הוראות חוק חופש המידע אינן מחייבות את הרשות הציבורית למסור מידע אלא באופן בו הוא שמור בידה. לפיכך מוצע לתקן את ההוראה הקיימת כך שבעל המאגר ימסור את המידע בשפה בה המידע שמור, כל עוד זו שפה מובנת ובלבד שאינה "שפה" כהגדרתה בחוק המחשבים.

8.3.4 - המלצת הצוות

מוצע לתקן את סעיף 13(ב) באופן הבא – **במקום "העברית, הערבית או האנגלית" יבוא** **"בה שמור המידע ובלבד שאינה "שפה קריאת מחשב" כהגדרתה בחוק המחשבים, התשנ"ה-1995."**

8.4 – זכות התיקון

8.4.1 - המצב הקיים

> "14. (א) אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ - למחזיק מאגר המידע, בבקשה לתקן את המידע או למוחקו.
>
> (ב) הסכים בעל מאגר המידע לבקשה כאמור בסעיף קטן (א) יבצע את השינויים הנדרשים במידע שברשותו ויודיע עליהם לכל מי שקיבל ממנו את המידע בתקופה שנקבעה בתקנות.
>
> (ג) סירב בעל מאגר המידע למלא בקשה כאמור בסעיף קטן (א) יודיע על כך למבקש, באופן ובדרך שנקבעו בתקנות.
>
> (ד) מחזיק חייב לתקן מידע, אם בעל מאגר המידע הסכים לתיקון המבוקש או שבית משפט ציווה על התיקון."

8.4.2 - משפט משווה

8.4.2.1 – קנדה

חוק הפרטיות הקנדי מעגן את זכותו של מושא המידע לתקן מידע אודותיו בסעיף 12(2) לחוק. הוראות החוק קובעות כי תצוין הערה ליד מידע שנתבקש שינויו אולם הוא לא שונה (סעיף 12(2)(b) לחוק הפרטיות) וכן כי כל גוף שהועבר אליו מידע למטרה אדמיניסטרטיבית[57] בשנתיים האחרונות יודיעו לו על התיקון (סעיף 12(2)(c) לחוק הפרטיות).

ב-PIPEDA זכות התיקון מעוגנת כך שכאשר הפרט מוכיח אי דיוק ברישום המידע אצל בעל המאגר, על בעל המאגר לתקן את המידע ולהודיע על התיקון לצדדים שלישיים שיש להם גישה למידע (סעיף 4.9.5 לנספח). גם ב-PIPEDA, בדומה לחוק הפרטיות הקנדי, ישנה התייחסות למקרה בו המידע אינו מתוקן לפי בקשת מושא המידע (סעיף 4.9.6 לנספח).

8.4.2.2 – האיחוד האירופי

מכיוון שהדירקטיבה האירופית מחייבת את בעלי מאגר המידע לשמור על מידע מדויק ועדכני, "זכות התיקון" מנוסחת כ"חובת התיקון" החלה על בעלי המאגר לצורך עמידה בתנאי הדירקטיבה (סעיף 12(b) לדירקטיבה). גם בדירקטיבה יש חובה להעביר את המידע המתוקן לצדדים שלישיים אלא אם הוכח כי הדבר בלתי אפשרי או כרוך במאמצים בלתי סבירים (סעיף 12(c) לדירקטיבה).

8.4.2.3 – אירלנד

חוק הגנת המידע באירלנד מחייב את בעל מאגר המידע להגיב תוך 40 יום לבקשה לתיקון או מחיקת מידע. החובה לעדכן צדדים שלישיים אודות התיקון שבוצע היא לאותם צדדים שהמידע הועבר אליהם ב-12 החודשים שקדמו לתיקון שבוצע (סעיף 6 לחוק הגנת המידע).

---

[57] כך לשון החוק: "for use for an administrative purpose"

<u>8.4.3 – הסכמה כללית</u>

כפי שמצוין לעיל, זכות התיקון מוכרת על ידי שיטות משפט נוספות. חשיבותה של זכות זו היא במעמד שניתן למושא המידע כמי שיכול להבטיח כי מידע אודותיו המצוי בידיים אחרות יהיה נכון ועדכני. אלמלא זכות התיקון, זכות העיון הייתה חסרה בכך שמושא המידע יכול היה להיחשף למידע אודותיו ללא יכולת להתגונן מול מידע לא מדויק.

<u>8.4.4 – המלצת הצוות</u>

אין צורך בתיקון חקיקה.

8.5 – מאגרים שאינם פעילים

אגב הדיון בצוות בזכויות העיון והתיקון, עלה נושא נוסף הנוגע להיקף החובה שיש להטיל על מאגרי מידע שאינם פעילים. לפיכך הצוות דן בזכות העיון והתיקון במאגרים שאינם פעילים, מאגרי מידע שאינם משמשים את בעל המאגר או מי שנהנה ממנו במהלך עסקיו הרגילים. לדוגמא, מאגרים ישנים שאינם מחוברים לרשת של בעל העסק.

8.5.1 - דעת הרוב

לדעת מרבית חברי הצוות אין להקנות זכות עיון ותיקון במאגרי מידע שאינם פעילים. הטעם לכך הוא שזכויות אלו נועדו לאפשר למושא המידע לדעת מהו המידע הקיים אודותיו במאגר ומשמש את בעל מאגר המידע לצורך קבלת החלטות לגביו, ולתקן מידע זה במידה שהמידע אינו מדויק. מיותר לציין כי במידה שמאגר לא פעיל יופעל שוב, הריהו יחשב למאגר מידע לכל דבר ועניין. מובן, כי אף אם אין זכות עיון במאגר מידע שכזה, אין הדבר גורע מחובת בעל המאגר ומחזיק המאגר בכל הקשור לאבטחת המידע.

8.5.2 - דעת מיעוט[58]

לדעת מיעוט חברי הצוות כל עוד מאגר קיים ולא בוער, מאגר המידע הוא בעל ערך לבעליו ועל כן יש לאפשר למושאי מידע לעיין ולתקן את המידע המצוי במאגר. מאגרים לא פעילים, לעתים, הם בעלי סיכון גבוה יותר מכיוון שהעובדה שאינם משמשים את הבעלים באופן שוטף גורמת לכך שההקפדה על נהלי אבטחת המידע במאגר פוחתים ועל כן החשש כי יעשה שימוש לרעה במידע המצוי במאגר – גובר.

8.5.2.3 - המלצת הצוות

מוצע להבהיר כי זכויות העיון והתיקון חלות רק על מאגרי מידע פעילים.

[58] יובל אלוביץ', עומר טנא, נחמן ליס ובובי פיינדריך

9 – פטור למאגרים מיוחדים מזכות העיון ומחובת ההודעה

9.1 – פטור ממתן זכות עיון

9.1.1 - המצב הקיים

סעיף 13(ה) קובע כי זכות העיון, אשר זכות התיקון נגזרת ממנה, אינה חלה על המאגרים שבידי הגופים הבאים:

1. משטרת ישראל, אגף המודיעין במטכ"ל, המשטרה הצבאית, השב"כ והמוסד (סעיף 13(ה)(1) לחוק);
2. שירות בתי הסוהר (סעיף 13(ה)(1א) לחוק);
3. רשות המסים (סעיף 13(ה)(2) לחוק);
4. משרד הביטחון, הרשות לפיתוח אמצעי לחימה (רפא"ל), התעשייה הצבאית, התעשייה האווירית לישראל, חברות בת שלה ויחידות תפעול שלה – ובלבד שאדם המבקש לעיין במידע שעליו יהיה זכאי לעיין במידע שאינו מידע סודי (סעיף 13(ה)(4) לחוק והתקנות מכוחו[59]);
5. מח"ש - אודות חקירות ואכיפת החוק, הרשות לניירות ערך והרשות להגבלים עסקיים - אודות חקירות בלבד (סעיף 13(ה)(5) לחוק והצו מכוחו[60]).

כמו כן קיים פטור ממתן זכות עיון כאשר בטחון המדינה, יחסי החוץ שלה או הוראות חיקוק מחייבים שלא לגלות מידע למושא המידע (סעיף 13(ה)(3) לחוק).

9.1.2 - משפט משווה

9.1.2.1 – קנדה

חוק הפרטיות מעגן את הפטור מזכות העיון מסיבות שונות, ביניהן:

1. חשיפת המידע צפויה לפגוע ביחסי החוץ, בהגנה על קנדה או על כל מדינה שהיא בעלת ברית או קשורה לקנדה, במאמציה של קנדה להתחקות, למנוע או לדכא חתרנות או פעולות איבה (סעיף 21 לחוק הפרטיות);
2. מידע שהושג או הוכן על ידי רשויות חקירה לצרכי חקירה או אכיפה אם חלף פחות מ-20 שנה ממועד יצירת המידע (סעיף 22 לחוק הפרטיות) ;
3. בטחון הציבור עלול להיפגע (סעיף 25 לחוק הפרטיות).

כמו כן מונה החוק מספר חסינויות בגינן לא ניתן למסור מידע – כגון חיסיון עו"ד לקוח (סעיפים 26-28 לחוק הפרטיות).

לפי סעיף 9 ל-PIPEDA, לא יימסר מידע אשר יש בו כדי לחשוף מידע אישי אודות צד ג'. מלבד זאת, סעיף 4.9 בנספח לחוק מאפשר אי מסירת מידע לפי שיקול דעתו של כל ארגון בתנאי ששיקול הדעת יהיה ברור, ספציפי ומנומק לגבי המקרים בהם לא יימסר מידע.

---

59 תקנות הגנת הפרטיות (קביעת מאגרי מידע הכוללים מידע שלא לגילוי), התשמ"ז-1987 - פורסם בק"ת התשמ"ז, עמ' 754.

60 צו הגנת הפרטיות (קביעת רשות חקירה), התשנ"ח-1998 - פורסם בק"ת התשנ"ח, עמ' 604.

9.1.2.2 – האיחוד האירופי

כפי שצוין בתחילת הדו"ח[61], הדירקטיבה כלל אינה חלה על עיבוד מידע הנוגע, בין היתר, לביטחון הציבור, להגנת המדינה ובטחונה ולתחום המשפט הפלילי (סעיף 3(2) לדירקטיבה), על אף שמדינות אירופיות רבות המאמצות את הוראות הדירקטיבה לדין המקומי, מרחיבות את תחולתו גם על תחומים אלו, כך שקיימים פטורים הדומים במהותם, גם אם לא בהיקפם, לאלה בסעיף 13(ה).

נוסף על הוצאת תחומים שונים מתחולת הדירקטיבה, האיחוד האירופי מאפשר למדינות חברות האיחוד לחרוג מזכות העיון כאשר ההחרגה קשורה לאחד מהנושאים המנויים בסעיף 13(1) לדירקטיבה. הנושאים מתייחסים בין היתר לביטחון הלאומי (סעיף 13(1)(a) לדירקטיבה), לביטחון הציבור (סעיף 13(1)(c) לדירקטיבה), מניעה, חקירה, חשיפה ותביעה בעבירות פליליות או בהפרה של כללי אתיקה של מקצועות מוסדרים (סעיף 13(1)(d) לדירקטיבה) ואינטרס כלכלי או פיננסי חשוב של אחת ממדינות האיחוד (סעיף 13(1)(e) לדירקטיבה).

כמו כן, מאפשר האיחוד להחריג, באופן מסודר בחקיקה, מאגרים שנועדו לצרכי מחקר או סטטיסטיקה בלבד (סעיף 13(2) לדירקטיבה).

9.1.2.3 – אירלנד

חוק הגנת המידע באירלנד, בנוסף להטמעת החריגים המצויים בדירקטיבה האירופית (סעיף 5(1) לחוק הגנת המידע), מוסיף מספר הוראות ייחודיות –

1. לא יימסר מידע במקום בו מסירת המידע סביר כי תפגע בביטחון או בסדר הטוב ובמשמעת בבתי כלא (סעיף 5(1)(c) לחוק הגנת המידע);
2. המידע המבוקש נמצא בידי נציב הפרטיות או נציב המידע לצורך מילוי תפקידו (סעיף 5(1)(gg) לחוק הגנת המידע);
3. המידע נמצא במערכת גיבוי (סעיף 5(1)(i) לחוק הגנת המידע).

<u>9.1.3 – הסכמה כללית</u>

במהלך פעילות הצוות נעשתה פניה ראשונית לגופים המנויים בסעיף 13(ה) בה נאמר כי בדעת הצוות לצמצם את הוראות סעיף 13(ה) כך שיתאים להוראות חוק חופש המידע. כוונת הצוות הייתה לדון עם כל הגופים הרלוונטים על מנת ללבן את עמדתם של גופים אלו ולהבין את הקושי בצמצום הפטור הקיים היום בחוק הגנת הפרטיות אף מעבר להתאמתו להוראות חוק חופש המידע. מכיוון שלא כל הגופים הנוגעים בדבר השיבו לפנייתנו במועד, נבצר מהצוות לקיים דיון מעמיק בסוגיה. לפיכך על אף שחברי הצוות סבורים כי יש מקום לבחון צמצום נוסף בפטור, הוחלט שהמלצה כאמור לא תצא מאת הצוות וזאת מהטעם שלא נשמעה עמדתם המקצועית של הגופים הרלוונטים.

לגופו של עניין, חוק חופש המידע מחייב רשויות ציבוריות, כהגדרתן באותו חוק, להיענות לבקשות לקבלת מידע מאת הציבור, אלא אם מתקיימות אחת העילות המנויות בסעיפים 8 ו-9

[61] בפרק 1.3.2

לחוק אשר אוסרים או מאפשרים לרשות שלא למסור מידע על מנת להגן על אינטרסים אחרים כגון בטחון המדינה[62], הגנת הפרטיות[63], סודות מסחריים[64] ועוד. כמו כן מונה חוק חופש המידע רשימה של גופים אשר חוק חופש המידע אינו חל עליהם[65]. בדברי ההסבר להצעת החוק מוסבר כי בגופים מסוימים, מתן מענה כי חומר מסוים הנו חסוי מהווה אינדיקציה לכך שחומר כאמור קיים ובכך עלול להיגרם נזק לעניין חיוני. לדוגמא, העובדה שהמשטרה מנהלת חקירה נגד פלוני - עובדה זו כשלעצמה עלולה להיות חסויה על מנת לא לסכל את החקירה.

מטרתו של חוק חופש המידע הוא להגביר את השקיפות ברשויות הציבוריות וזאת על מנת שהציבור יוכל לבקר את מעשיהם מתוך הנחה כי הרשויות הן שלוחיו של הציבור. לעומת זאת, מטרתה של זכות העיון המעוגנת בחוק היא לאפשר לאדם לדעת מי מחזיק במידע אודותיו, לאלו מטרות ומהו תוכן המידע המוחזק. האינטרס הפרטי של אדם לבקר את אלו שמחזיקים במידע אודותיו גדול, לכאורה, מהאינטרס של הציבור לקבל מידע מהרשויות הציבוריות לצורך ביקורת עליהם.

כפי שצוין לעיל, מכיוון שנבצר מהצוות לקיים דיון ענייני עם הגופים הרלוונטים בצמצום הוראות סעיף 13(ה), הוחלט להמליץ כי עד שיתקיים דיון ממצה בנושא, ועל מנת ליצור אחידות בין דברי החקיקה השונים, יצומצם הפטור בסעיף 13(ה) לחוק ויותאם לפטורים בחוק חופש המידע. לדעת הצוות, מקום בה רשות ציבורית מחויבת לתת מידע לכלל הציבור, אין לפטור אותה ממתן מידע על אדם שמידע אודותיו מצוי בידה היות שהאינטרס שלו בקבלת המידע גדול מהאינטרס של מבקש המידע לפי חוק חופש המידע.

כמו כן ממליץ הצוות כי בעתיד הקרוב יתנהל דיון עם הגופים הרלוונטים על מנת לבחון צמצום נוסף של הפטור בסעיף 13(ה) לחוק.

9.1.4 - המלצת הצוות

1. הפטור מזכות העיון יותאם לפטורים ממסירת מידע לפי חוק חופש המידע.

2. צמצום נוסף של הפטור מזכות העיון יבחן בקרוב מול הגופים הרלוונטים.

[62] סעיף 9(א)(1) לחוק חופש המידע
[63] סעיף 9(א)(3) לחוק חופש המידע
[64] סעיף 9(ב)(6) לחוק חופש המידע
[65] סעיף 14 לחוק חופש המידע

9.2 - פטור ממתן הודעה

9.2.1 - המצב הקיים

כיום, חובת מתן ההודעה חלה על כל מי שאוסף מידע לצורך החזקתו או שימוש בו במאגר מידע, ללא פטור.

9.2.2 – הסכמה כללית

לדעת הצוות אין לתת פטור גורף לגופים המנויים בסעיף 13(ה) מחובת ההודעה. העובדה שזכות העיון אינה מוקנית למושא המידע במקרים מסוימים, אינה פוטרת את אוסף המידע למסור לידיעת האדם עליו נאסף המידע מספר נתונים שיאפשרו לו לבקר, גם אם באופן מוגבל, את אוסף המידע.

מוצע כי אוסף מידע למאגרים המנויים בסעיף 13(ה), לא יהיה פטור ממתן הודעה אלא אם מתן ההודעה, או פרט מפריטי ההודעה, עלול לסכל את המטרה לשמה נאסף המידע.

9.2.4 - המלצת הצוות

מוצע לתקן את החוק כך שגופים המנויים בסעיף 13(ה) יהיו פטורים ממתן הודעה לפי סעיף 11 לחוק רק אם מתן ההודעה עלול לסכל את המטרה לשמה נאסף המידע.

10 - דיוור ישיר

"17ג. **הגדרות**
בסימן זה -
"דיוור ישיר" - פניה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי איפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע;
"פניה" - לרבות בכתב, בדפוס, בטלפון, בפקסימליה, בדרך ממוחשבת או באמצעי אחר;
"שירותי דיוור ישיר" - מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא."

בטרם נדון בסוגיות בתחום זה נעיר כי, בכל הנוגע לדיון בדיוור ישיר, הצוות מודע לכך שישנה משמעות מוגבלת להסדרים אותם אנו מציעים ככל שהדיוור הישיר מתבצע באמצעים אלקטרונים שמקורם בחו"ל. ניסיון להתמודד עם דיוור ישיר שמקורו מחוץ לגבולות הארץ, יכול להתבצע רק באמצעות שיתוף פעולה בינלאומי, שלעת עתה, אינו קיים.

10.1 – דיוור ישיר

השאלה שעמדה על הפרק היא האם לצורכי דיוור ישיר נדרוש מבעל המאגר שההסכמה להיכלל במאגר צריכה להיות מפורשת (opt in), או שמא ניתן להסתפק באי הבעת התנגדות של מושא המידע, תוך מתן אפשרות להודיע על רצונו להיגרע מהמאגר (opt out).

10.1.1 - המצב הקיים

החוק הקיים מאפשר לבצע דיוור ישיר בין באופן ישיר ובין באמצעות שרותי דיוור ישיר על אף שלא ניתנה הסכמה מראש. מי שמעוניין במחיקתו ממאגרים ממין זה זכאי לפנות לבעל המאגר לשם מחיקתו. ההסדר מעוגן בסעיף 17ו שלשונו –

"17ו(ב) כל אדם זכאי לדרוש, בכתב, מבעל מאגר מידע המשמש לדיוור ישיר, שמידע המתייחס אליו יימחק ממאגר המידע.

(ג) כל אדם זכאי לדרוש, בכתב, מבעל מאגר המידע המשמש לשירותי דיוור ישיר או מבעל מאגר המידע שבו מצוי המידע שעל-פיו בוצעה הפניה, כי מידע המתייחס אליו לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים, והכל לפרק זמן מוגבל או קבוע.

(ד) הודיע אדם לבעל מאגר המידע על דרישתו כאמור בסעיפים קטנים (ב) או (ג), יפעל בעל המאגר בהתאם לדרישה ויודיע לאדם, בכתב, כי פעל על פיה."

בימים אלו נדונה הצעת חוק התקשורת (בזק ושידורים) (תיקון מס' 33), התשס"ה-2005[66] (להלן – **הצעת חוק התקשורת**), בוועדה המשותפת לועדת הכלכלה ולוועדת המדע והטכנולוגיה בכנסת,

[66] פורסם בה"ח הממשלה התשס"ה, עמ' 886

בניסיון להתמודד עם תופעת ההפצה ההמונית של הודעות פרסומת בלתי רצויות הנשלחות באמצעים אלקטרוניים. ההצעה מאמצת את ההסדר של האיחוד האירופי ודורשת כי פניות כאמור תוכלנה להיעשות רק אם תינתן הסכמה מראש של הנמען. להלן הנוסח המוצע -

> "30א(א) לא ישגר מפרסם דבר פרסומת באמצעות פקסימילה, מערכת חיוג אוטומטי, הודעת דואר אלקטרוני או הודעת מסר קצר, בלא קבלת הסכמה מפורשת מראש של הנמען; פניה חד פעמית מטעם מפרסם לנמען שהוא בית עסק, באחת הדרכים האמורות בסעיף קטן זה, המהווה הצעה להסכים לקבלת דברי פרסומת מטעמו, לא תחשב הפרה של הוראות סעיף זה. "

הצוות בחן את ההסדר הרצוי בחוק הגנת הפרטיות, מתוך הנחה שההסדר המוצע בחוק התקשורת יתקבל ויהפוך לחוק. נציין כי ההבדל בין שני החוקים, נוסף על דרישת ההסכמה מראש, הוא כי הצעת חוק התקשורת מתייחסת רק <u>לפרסום</u> שנעשה <u>באמצעים</u> <u>מסוימים</u> בעוד חוק הגנת הפרטיות אינו מתייחס לתוכן הפניה ולטכנולוגיה בה נעשה שימוש אלא רק לעובדה כי הפניה (לרבות בפניה בדואר רגיל) נעשתה תוך שימוש במאגר דיוור ישיר המבוסס על חתך מאפיין של כל הנמענים.

<u>10.1.2 - משפט משווה</u>

ככלל, מדינות שונות החילו בשנים האחרונות הוראות הנוגעות לתחום דואר הזבל האלקטרוני (Spam). עם זאת אין התייחסות הדומה להסדר הישראלי בחוק הגנת הפרטיות המסדיר פניה על בסיס חתך מאפיין. להלן שתי דוגמאות להסדר בתחום הדואר זבל.

10.1.2.1 – האיחוד האירופי

כפי שציינו לעיל, הצעת חוק התקשרות בנושא דואר זבל העתיקה את ההסדר של האיחוד האירופי המצוי בסעיף 13 לדירקטיבה 2002/58/EC שעניינה פרטיות ותקשורת אלקטרונית[67]. האיחוד אוסר על שימוש במערכות תקשורת אוטומטיות אלא אם התקבלה מראש הסכמתו של הנמען (opt in) וזאת למעט במקרים חריגים.

10.1.2.2 – אוסטרליה

בשנת 2003 נחקק באוסטרליה ה- Spam Act. החוק קובע כי אין לשלוח הודעות מסחריות בדואר אלקטרוני, ב-SMS, ב-MMS או בתוכנות מסר מיידי (instant messaging) אלא אם התקבלה הסכמה מראש של אותו אדם לקבלת המידע (סעיף 15 לחוק).
בנוסף, החוק האוסטרלי אף אוסר על שימוש בתוכנות לאיסוף כתובות וכן שימוש ברשימות תפוצה שהוכנו תוך שימוש בתוכנות איסוף (סעיף 19 לחוק).

---

67 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

10.1.3 – דעת הרוב

מרבית חברי הצוות סבורים שיש ליצור הסדר משולב בו משלוח דואר באמצעים שעלותם זניחה למפרסם תדרוש הסכמה מראש (opt in) כפי שמוצע בהצעת חוק התקשורת, ואילו משלוח דואר באמצעות דואר רגיל או באמצעות טלמרקטינג, יאפשרו לנמען לדרוש את הוצאתו מהמאגר (opt out).

ההסדר המשולב נועד, לשיטתם, ליצור קוהרנטיות בין הוראות חוק התקשורת לבין הוראות חוק הגנת הפרטיות כפי שמוצע בהסדר של האיחוד האירופי. כמו כן ההצעה מכירה בחשיבות של מתן אפשרות לפנות לחתך אוכלוסיה מסוים, עם מתן אפשרות לנמען לבקש שלא ישלחו לו בעתיד מידע נוסף.

10.1.4 – דעת מיעוט[68]

מיעוט חברי הצוות סבורים כי בטרם ביצוע דיוור ישיר יש צורך בקבלת הסכמת מושא המידע, וזאת עם הכנסת פרטיו למאגר המידע המשמש לדיוור ישיר (opt in). לשיטתם, בשל העובדה כי דיוור ישיר מתבסס על אפיון מסוים המשותף לכל הנמענים ובכך הרכבת הרשימה והפצתה פוגעות בפרטיות - יש צורך בהסכמה מלכתחילה לביצוע דיוור ישיר.

10.1.5 - המלצת הצוות

מוצע כי החוק הקיים יתוקן כך שהוא חל רק על אותם מקרים שחוק התקשורת אינו חל עליהם.

[68] עמית אשכנזי, מיכאל בירנהק ואבנר פינצ'וק

10.2 – אבחנה בין שרותי דיוור ישיר לדיוור ישיר

10.2.1 - המצב הקיים

החוק מבחין בין שרותי דיוור ישיר לדיוור ישיר בשלושה עניינים –

1. בעל מאגר לשרותי דיוור ישיר חייב להיות רשום בפנקס כאמור בסעיף 17ד לחוק:

> "17ד. לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן הוא רשום בפנקס ואחת ממטרותיו הרשומות היא שירותי דיוור."

2. מנהל המאגר או מחזיקו צריך שיהיה בידו ציון מקורות המידע כאמור בסעיף 17ה לחוק:

> " 17ה. לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן יש בידו רישום המציין את המקור שממנו קיבל כל אוסף נתונים המשמש לצורך מאגר המידע ומועד קבלתו, וכן למי מסר כל אוסף נתונים כאמור."

3. לפי סעיף 17ו(ב) אדם זכאי לדרוש כי מידע אודותיו ימחק ממאגר מידע <u>המשמש</u> לדיוור ישיר, בעוד במידה שהמידע אודותיו שמור במאגר מידע <u>לשרותי</u> דיוור ישיר, זכותו לדרוש כי מידע אודותיו לא יימסר לאחר (סעיף 17ו(ג) לחוק).

10.2.2 – דעת הרוב

לדעת מרבית חברי הצוות החשש מפגיעה בפרטיות מתגבר בהתייחס למאגר מידע המשמש לדיוור ישיר אשר יוצר חתכים של קבוצות בני אדם לפי מאפיין מסוים, ומידע זה נמסר לאחר לצורך דיוור ישיר. העובדה שבעלי עסקים לשרותי דיוור ישיר אוספים מידע רב וסוחרים בו, דורש הקפדה יתרה איתם ועל כן יש להשאיר את האבחנה הקיימת בחוק בין מאגר לשרותי דיוור ישיר למאגר המשמש לדיוור ישיר.

עם זאת מרבית חברי הצוות סבורים שיש לתקן את הוראות סעיף 17ו(ב) כך שהזכות להימחק ממאגר תהיה שמורה רק לגבי מאגר לשרותי דיוור ישיר, הסוחר במידע, ולא למאגר שאגב השימוש העיקרי בו, נעשה בו שימוש לצרכי דיוור ישיר[69].

---

[69] לדוגמא, ניתן לפנות לבעל המועדון בו הנמען חבר על מנת שלא ישלח חומר פרסומי, אולם הנמען אינו יכול לדרוש מבעל המועדון למחוק את פרטיו ממאגר המידע שבידו מכיוון שהפרטים דרושים לצורך פעילותו השוטפת.

10.2.3 - דעת מיעוט[70]

אין להבחין בין שרותי דיוור ישיר לדיוור ישיר מהטעם שהנמען אינו מבחין בין משלוח הודעה המתבססת על דיוור ישיר לבין זו המתבססת על שרותי דיוור ישיר, בהתייחס לשימוש שנעשה במידע אודותיו. ככל שקיים מאגר עיקרי, המשמש בין היתר לדיוור ישיר או לשרותי דיוור ישיר, יש לחייב הקמה ורישום של מאגר נפרד שמטרתו דיוור ישיר או מתן שרותי דיוור ישיר, כך שהנמען יוכל לבקש הסרה מרשימת התפוצה ללא תלות בשימוש במידע הנדרש לצורך ניהול המאגר העיקרי.

10.2.4 - המלצת הצוות

אין צורך בתיקון חקיקה למעט תיקון 17ו(ב) כך שניתן יהיה להפנות דרישה למחיקת המידע ממאגר לשרותי דיוור ישיר ולא תינתן אפשרות למחיקה ממאגר המשמש בין היתר לדיוור ישיר.

[70] נחמן ליס ואבנר פינצ'וק

11 - העברת מידע לחו"ל

11.1 – העברת מידע לחו"ל

11.1.1 - המצב הקיים

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001[71] נועדו לאפשר לישראל לעמוד בסטנדרטים שקבע האיחוד האירופי לשם הכרה בה כמדינה שלישית שניתן להעביר אליה מידע מחוץ לאיחוד.

התקנות קובעות מספר הסדרים הכוללים –

1. הגבלת העברתו של מידע מחוץ לישראל אלא אם המידע מועבר למדינה המבטיחה רמת הגנה שאינה פחותה מרמת ההגנה בישראל (תקנה 1);
2. תנאים אשר בהתקיימם ניתן להעביר מידע לחו"ל על אף האמור בתקנה 1 (תקנה 2);
3. קבלת התחייבות בכתב להבטחת הפרטיות מאת בעל המאגר אליו מועבר המידע (תקנה 3);
4. קביעה שהוראות התקנות לא יחולו על העברת מידע עקב בקשה לפי חוק עזרה משפטית בין מדינות, התשנ"ח-1998 .

11.1.2 – משפט משווה

11.1.2.1 - האיחוד האירופי

סעיף 25 לדירקטיבה קובע הסדר בו מדינות שתהיינה מוכרות על ידי הנציבות כמדינות בהן ההסדר החוקי תואם את הוראות הדירקטיבה, ניתן יהיה להעביר אליהן מידע. נציין כי המדינות שהוכרו עד למועד פרסום הדו"ח כמדינות התואמות את ההסדר האירופי הן: ארגנטינה, קנדה, שוויץ, גרנזי והאי מאן.

נציין כי ארה"ב לא הוכרה כמדינה עם הגנה הולמת, אך לנוכח מעמדה הפוליטי והכלכלי הגיעה להסכם פרטני עם הנציבות, שלפיו אפשר יהיה להעביר מידע מאירופה אל חברות אמריקניות המצהירות כי הן מקיימות את עיקרי הדירקטיבה (הסדר ה-safe harbor).

סעיף 26 לדירקטיבה מאפשר העברת מידע למאגרי מידע המצויים במדינות שלא הוכרו בהתאם לסעיף 25, אולם רק בהתאם לתנאים המנויים בסעיף 26(1) לדירקטיבה. נציין כי ישנה אפשרות שמדינה מהאיחוד האירופי תסכים להעברת מידע למדינה שלא הוכרה כתואמת את הוראות הדירקטיבה וזאת בכפוף להטלת חסמים אשר יתרמו לשמירה על זכויות הפרט (סעיף 26(2) לדירקטיבה). במקרה ומדינה פעלה בהתאם לסעיף 26(2) עליה להודיע על כך לנציבות ולשאר מדינות האיחוד (סעיף 26(3) לדירקטיבה).

קודם לדירקטיבה, בשנת 1981, חתמו מדינות מועצת אירופה על אמנה להגנה על בני אדם בקשר לעיבוד אוטומטי של מידע אישי[72], שעיקריה אומצו בדירקטיבה. אף כי מדינות שאינן חברות

---

[71] ק"ת תשס"א, בעמ' 900

[72] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

במועצת אירופה יכולות להצטרף לאמנה, על פי ועדת השרים של המועצה (סעיף 23 לאמנה), עד למועד פרסום הדו״ח לא היו מדינות, למעט המדינות החברות במועצת אירופה, שהצטרפו לאמנה.

<u>11.1.3 – הסכמה כללית</u>

11.1.3.1 – העברת מידע ממדינות אחרות לישראל

חברי הצוות הסכימו כי יש לבחון האם אירופה מוכנה להכיר במדינת ישראל כמדינה המבטיחה רמת הגנה המתאימה לדרישות הדירקטיבה האירופית.

חברי הצוות סבורים, כי עדיפה ההכרה בהתאם לסעיף 25(2) לדירקטיבה על פני הצטרפות לאמנה, בעיקר בשל העובדה שבמסגרת הדירקטיבה כבר הוכרו מספר מדינות כממלאות אחר הסטנדרטים האירופים, בעוד שבאמנה חברים רק מדינות מועצת אירופה. לאור האמור הצוות רואה בעדיפות גבוהה ניסיון להיות מוכרים על פי הדירקטיבה, הכרה אשר תקנה לנו אפשרות להעביר מידע אף לאותן מדינות נוספות.

הדירקטיבה היא בעלת החשיבות העיקרית כיום, עקב יישומה בחקיקה מחייבת בכל מדינות האיחוד. לאמנה, לעומת זאת, חשיבות בעיקר בתחומים שאינם מכוסים על ידי הדירקטיבה (ביטחון לאומי, אכיפת חוק וכו׳).

נציין, כי בעקבות המלצת הצוות, פנה משרד המשפטים באמצעות משרד החוץ לנציבות האיחוד האירופי בנושא. בימים אלו מתקיימים מגעים מול האיחוד האירופי על מנת לברר את עמדתו בנוגע לבקשה של ישראל להיות מוכרת כמדינה התואמת את הדירקטיבה.

11.1.3.2 – העברת מידע מישראל למדינות אחרות

חברי הצוות הסכימו כי התקנות, בנוסחן היום, יוצרות חוסר בהירות בנוגע לגורם המוסמך להכיר בהעברת מידע מותרת לחו״ל, דבר הגורם לאי בהירות משפטית. לפיכך מוצע כי סמוך לאחר תיקון החקיקה הראשית יבחן משרד המשפטים תקנות אלו מחדש.

11.1.3.3 – סנקציה

חברי הצוות מציעים לקבוע סנקציה פלילית נגד מי שהעביר מידע למדינה זרה שלא כחוק. הצורך, לדעת חברי הצוות, בסנקציה פלילית היא שבשל המגבלה לאכוף את חוק הגנת הפרטיות מעבר לגבולות המדינה, ללא סנקציה – האיסור על העברת מידע לחו״ל יהיה חסר משמעות.

<u>11.1.4 - המלצת הצוות</u>

1. יש לבחון מחדש את נוסח התקנות הקיים;

2. יש לקבוע כי העברת מידע לחו״ל שלא בהתאם לתקנות מהווה עבירה פלילית וזאת בכפוף להבהרת התקנות כך שהאיסור יהיה ברור.

12 – סיכום

12.1 - תמצית החלטות הצוות

לסיכום, להלן תמצית המלצות הצוות כסדרן –

2 - היקף התחולה של פרק ב׳

1. אין להחיל את החוק על תאגיד כנפגע;
2. ״מאגר מידע״ יוגדר כ״אוסף של נתוני מידע אישי שניתן לאתר מידע המצוי בו לפי אפיון או חתך מסוים״;

3 - הגדרות

3. במקום הגדרת ״מידע״ יוגדר המינוח ״מידע אישי״ כ״כל מידע אודות אדם מזוהה או הניתן לזיהוי באמצעים סבירים״;
4. בעתיד יש לבחון שימוש במונחים אחידים המתייחסים ל״פרטיות״;
5. הגדרת ״מידע רגיש״ תמחק ובמקומה יוגדר כי מאגר מידע החייב ברישום הוא מאגר הכולל מידע מסוג מסוים;

4 - חובת הרישום

6. יש לצמצם את חובת הרישום כך שתחול בהתקיים אחת מהנסיבות הבאות -
   א. כאשר בעל המאגר ״סוחר״ במידע שברשותו;
   ב. כאשר המאגר כולל מידע רגיש.
7. יש להרחיב את סעיף 8(ה) כך שלרשם תהיה סמכות גם לחייב מאגר ברישום, על אף שהוא פטור;
8. יש להוסיף הוראה כי שר המשפטים יהיה רשאי להורות לחייב או לפטור סוג מאגרים מסוים מרישום;

5 - סמכויות הרשם

9. יש להוסיף על סמכויותיו הקיימות של רשם מאגרי מידע, את הסמכויות או הנושאים הבאים -
   א. עצמאות שיקול הדעת של הממונה על מאגרי המידע ובכלל זה סמכותו להתייצב בהליך משפטי שיש בו עניין ציבורי הנוגע למילוי הוראות פרק ב׳ לחוק;
   ב. קביעת הנחיות בנוגע לאופן ניהול מאגר מידע ומילוי ההוראות לפי פרק זה;
   ג. מתן סמכות לממונה לבחון תלונות שהופנו אליו בנוגע להפרה של הוראות פרק זה ולצורך בירור התלונות רשאי הממונה להורות על ביצוע פעולות פיקוח בהתאם להוראות סעיף 10(ה1) לחוק;
   ד. מתן סמכות לממונה להוציא צו אבטחת מידע בהתאם להמלצות הצוות בעניין אבטחת מידע.
10. יש לתקן את חוק תובענות ייצוגיות כך שהחוק הגנת הפרטיות יהיה מהחוקים שהפרתם מאפשרת הגשת תובענה ייצוגית.

6 - המועצה להגנת הפרטיות

11. יש לעגן בחקיקה את תפקידי המועצה, אופן מינויה והרכבה ;

7 - חובות הנלוות לניהול מאגר

12. אין להטיל על בעל מאגר מידע חובות מקדמיות לניהול מאגר מידע ;
13. מוצע לתקן את סעיף 11 כך שבחובת ההודעה יכללו גם הפרטים הבאים :
    א. מקור החובה החוקית לאיסוף המידע, במידה שישנה חובה כזו ;
    ב. פרטים על זכויות מושא המידע ביחס למידע שנאסף ממנו ;
    ג. פרטי דרכי ההתקשרות עם מבקש המידע.
14. יש לאסור העברת חתך רחב של מידע אישי לגורם אחר למטרה אחרת מהמטרה לשמה נדרש המידע אלא אם נתקבלה הסכמתו של מי שאודותיו נתבקש המידע להעברת המידע או אם המידע הועמד לעיון הציבור ;
15. יש להחליף את סעיף 17 לחוק כמוצע בסעיף 7.4.4.1 לדו"ח ;
16. יש להקנות סמכות לרשם מאגרי המידע לתת צווים אישיים ;
17. יש לשקול אימוץ של ההסדר הקליפורני לעניין כשל באבטחת מידע ;
18. אין להבחין בין מאגרים ממשלתיים לפרטיים לעניין חובת אבטחת המידע ;
19. יש לתקן את סעיף 16 לחוק כמוצע בסעיף 7.5.3 דו"ח ;

8 - זכות העיון והתיקון

20. יש להרחיב את זכות העיון לקבלת מידע נוסף כמפורט בסעיף 8.1.4 לדו"ח ;
21. יש לתקן את החוק כך שיפורסם מחיר העלות המקסימאלי למימוש זכות העיון. בעל מאגר אשר יבקש לגבות מחיר העולה על הסכום שנקבע, יצטרך לפנות לרשם על מנת שיאשר את המחיר החריג. לאחר שהפניה של בעל המאגר תובא לידיעת הציבור, הרשם יפרסם את החלטתו המנומקת ברבים.
22. יש להסדיר מחדש את תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון) ;
23. יש לתקן את סעיף 13(ב) כך שלא תוטל אחריות על בעל מאגר מידע לתרגם מידע שהועבר למושא המידע כמוצע בסעיף 8.3.4 לדו"ח ;
24. יש להבהיר כי זכויות העיון והתיקון חלות רק על מאגרי מידע פעילים ;

9 - פטור מזכות העיון

25. יש להתאים את הפטור מזכות העיון להוראות חוק חופש המידע ;
26. יש לבחון בקרוב, מול הגופים הרלוונטים, צמצום נוסף של הפטור ;
27. יש לתקן את החוק כך שגופים המנויים בסעיף 13(ה) יהיו פטורים ממתן הודעה לפי סעיף 11 לחוק אם מתן ההודעה עלול לסכל את המטרה לשמה נאסף המידע ;

10 - דיוור ישיר

28. מוצע כי החוק הקיים יתוקן כך שהוא חל רק על אותם מקרים שחוק התקשורת אינו חל עליהם ;
29. יש לתקן את סעיף 17ו(ב) לחוק כך שניתן יהיה להורות על מחיקת פרטים ממאגר המשמש לשרותי דיוור ישיר ;

11 - העברת מידע לחו״ל

30. יש לבחון מחדש את נוסח התקנות להעברת מידע לחו״ל ;
31. יש לקבוע כי העברת מידע לחו״ל שלא בהתאם לתקנות מהווה עבירה פלילית ;

<u>12.2 – סוף דבר</u>

עם הגשת הדו״ח, סיים צוות מאגרי המידע את מלאכתו. עם זאת, אנו רואים בכך את תחילתו של השיח הציבורי בנושא הסדרה מחודשת של תחום מאגרי המידע כפי שעלה מעבודת הצוות.

נציין כי לקראת סיום עבודת הצוות הועברה אלינו הצעות לתיקון החוק, בין היתר בהיבט של אבטחת מידע על ידי האגודה הישראלית לאבטחת מידע. עם זאת, לאור העובדה כי המסמך לא נדון על ידי הצוות הוחלט כי ההתייחסות להצעת האגודה בתחום זה תתבצע על ידי משרד המשפטים תוך קידומו של תזכיר חוק הגנת הפרטיות כפי שהומלץ על ידי הצוות. בנוסף, לאחר סיום עבודת הצוות ובטרם פורסם דו״ח זה, הוקמה במשרד המשפטים הרשות למשפט ולטכנולוגיית מידע. רשות זו תידרש אף היא לסוגיה שנדונה בצוות, ותבחן את הצורך בתיקונים נוספים ככל שיידרשו.

נספח – 13

טכנולוגיה ופרטיות – משפט משווה*

מר יעקב וילון,

מחלקת ייעוץ וחקיקה

*** המסמך משקף את המצב הקיים נכון למועד יצירת המסמך – 23/10/03**

Israel Ministry of Justice

Memorandum

To : Yehoshua Schoffman
Dalit Dror
Rivki Dvash

From : Yacov Wilon

Re : Technology and Privacy (Comparative Law)

Date : October 23, 2003

This memorandum provides a comparative law discussion of technology and privacy issues. The ideas and information presented herein are intended to serve as an aid in considering legislative and regulatory reforms in Israel.

I. Introductory Matters

A. General Approach.

While researching technology and privacy issues, I have become acutely aware of the challenges inherent in formulating legislative guidance. At least three difficulties arise. First, the interaction of technology and privacy generates more legal issues than any one memorandum can specifically address. Second, although many important privacy laws have been enacted in recent years, they have not yet been fully implemented, so there is a shortage of empirical evidence showing what works and what doesn't work. Third, the continuing rapid advance of technology makes it difficult to provide guidance with long-term relevance.

To mitigate the effect of those difficulties, I will provide a conceptual overview and an organizational framework for privacy and technology issues that I hope will remain relevant despite continuing technological change. I will also avoid making overly specific legislative recommendations, instead making general recommendations and describing relevant considerations in the hope that they will continue to be relevant over time.

B. Emphasis on Newer Issues.

Some areas of privacy law are well-developed. For example, the question of when and how a police officer may obtain a warrant to search a private residence is not a new one. There is substantial legal and empirical history regarding law enforcement search and seizure. I will not provide detailed analysis of such issues, except to the extent that they are affected by new technology.

Other areas of privacy law are new and in flux. For example, when cellular telephones and pagers are turned on, the network provider keeps track of their geographical location. How may that information be used? Another example: many

people use the Internet and e-mail on their computers at work. Should employers be permitted to monitor their employees' e-mail and Internet use? Such newer issues will receive more detailed attention.

However, before reviewing recent technological and legislative developments, it is worth considering some historical definitions and conceptions of privacy, along with their legal implications and consequences. The next section will focus primarily on legal commentary and reform in the United States.

II. Conceptions of Privacy and Their Influence on United States Law

Scholars have defined privacy using legal, moral, religious, philosophical, sociological, anthropological, psychological, or other terms. Different definitions serve different purposes. Legal and public policy experts have not been able to agree on one definition that is sufficiently specific and non-controversial to support all of their privacy-related legislative efforts.

Nonetheless, it is useful to examine some of the more often-cited definitions, and to describe their influence on the development of privacy law, in order to provide a conceptual background. I rely here primarily on the work of U.S. scholars, who have generated a rich and various literature on the subject.[1]

A. The Right to be Let Alone: Privacy and Tort Law.

The impact of technological and social change on privacy is not a new issue. In the late 1800's U.S. newspapers, using new printing and photography methods, relied heavily on scandal and gossip to expand their readership. In a landmark Harvard Law Review article published in 1890, the legal scholars Samuel Warren and Louis Brandeis complained that:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[2]

---

[1] An excellent historical survey of conceptions of privacy may be found in Ken Gormley, *One Hundred Years of Privacy,* 1992 Wisconsin Law Review 1335 (1992). Gormley argues that no one definition is capable of encompassing the various privacy interests that require legal protection. See also Fred H. Cate, Privacy in the Information Age (1997), at 19-28, for a thoughtful discussion of privacy interests.

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harvard Law Review 193, 196 (1890).

Warren and Brandeis defined privacy simply as "the right to be let alone."[1] They argued that a person should possess the legal means to protect his "inviolate personality" against injuries to his "feelings" or "honor."[2] They recommended the creation of a new legal right to privacy, so that a person whose privacy had been violated could bring a tort action for damages.[3]

Over time, privacy-related tort law did develop in the U.S. While the rules established by different states at different times were not always consistent, by 1960 the eminent U.S. tort law scholar Richard Prosser was able to classify prevailing law into four widely accepted categories of privacy torts: intrusion, disclosure, false light, and appropriation.[4]

Intrusion involves a physical act that unreasonably invades another person's solitude or seclusion. A common example of intrusion is when a "Peeping Tom" peers into the windows of a private home.

Disclosure involves public disclosure of truthful information that a reasonable person would find embarrassing or offensive. Examples would include publication of unauthorized nude photographs or private medical information.

False light torts involve publicity that places a person in a false light in the public eye. Defamation, including slander and libel, are typical examples.

Appropriation involves the unlawful use of an individual's name or likeness. A common example is the unauthorized use of a famous person's likeness for marketing or advertising purposes.

Although it is more than a century old, Warren and Brandeis' definition of privacy as "the right to be let alone" continues to be quoted by legal scholars. The historical circumstances underlying Warren and Brandeis' analysis, and the ensuing development of privacy torts, help to illustrate a number of important aspects of the development of technology and privacy law.

Technological advances often raise privacy concerns, which in turn inspire countermeasures. Countermeasures may be legal, or technological, or both. Warren and Brandeis were alarmed by the "yellow press" propelled by advances in newspaper technology, and their writings contributed to the development of legal remedies for some abuses. A technological solution to privacy concerns was described by David Flaherty, the Privacy Commissioner for the Canadian province of British Columbia: in the late 1940's, when small towns still used communal telephone lines ("party lines") that allowed residents to pick up their telephone receivers and eavesdrop on their neighbors, the installation of private lines solved the problem.[5]

---

[1]Id. at 193, 195.
[2]Id. at 205, 197-98.
[3]Id. at 219.
[4]William L. Prosser, *Privacy*, 48 California Law Rev. 383 (1960); see also William L. Prosser & W. Page Keeton, Law of Torts, at 851-866 (1984 & Supp.1988).
[5]David H. Flaherty, *Some Reflections on Privacy and Technology*, 26 Manitoba Law Journal 219, 224 (1999).

However, not every new encroachment on privacy is countered by a legal or technological response. Despite Warren and Brandeis' influence on privacy law, they did not succeed in banishing gossip and scandal from the news media. While they were shocked by the "yellow press," we have grown used to it. Technological and social change sometimes alter public expectations of how much privacy we have a right to expect. Sometimes that is a good thing. For example, teenagers used to enjoy making anonymous harassing "crank" telephone calls to strangers. Now, with caller identification available to telephone subscribers, teenagers must find other diversions.

Historical developments also show that privacy is an amorphous concept with elastic boundaries. Sometimes it is easier to say what privacy is not, than what it is. Many privacy violations do not involve physical harm, economic harm, or any interest in property. Many (but not all) privacy violations involve emotional distress, especially embarrassment, and the law attempts to create an objective standard by punishing only that conduct that would embarrass or offend a reasonable person.

Thus, policymakers assessing the privacy implications of new technology should proceed cautiously. They should determine whether the new technology is creating substantial public concern about privacy. If public concern is not widespread, or not deeply felt, then new laws may not be necessary or advisable. Indeed, if new laws are enacted without substantial public support, they may end up not being effectively enforced. Rather, the new technology may eventually bring about a change in public expectations.

If new technology is indeed creating substantial public concerns about privacy, then policymakers should determine what steps the manufacturers or users are implementing or contemplating to address those concerns. If private-sector solutions are imminent, then investing government resources may be unnecessary or unproductive, except to the extent that they encourage or complement private efforts.

Finally, if new technology creates substantial public concerns that are not adequately addressed by the private sector, then new legislation may be required.

B. Information Privacy: The Right to Control Personal Information.

In my research I found that two definitions of privacy were cited much more than any others. The first is that of Warren and Brandeis. The second is that of U.S. political scientist Alan Westin, who in 1967 defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others."[6]

Concerns about information privacy arose partly from the rise of totalitarian governments in the 1930's. But even democratic governments have extended their social, economic, law enforcement and national security functions to ever-wider spheres of human activity, and they have collected vast amounts of personal information to perform those functions. In the 1950's government agencies began using computers to store and process personal information, and private-sector organizations soon followed.

[6] Alan Westin, Privacy and Freedom (1967).

In response to concerns about government secrecy and misconduct, the U.S. enacted the Freedom of Information Act of 1966 allowing individuals to obtain access to many government records.[7] The Act contains exemptions preventing individuals from obtaining certain types of sensitive personal information (i.e. medical or criminal records) regarding other individuals.[8]

Similar concerns spurred the U.S. to enact of the Privacy Act of 1974, which obligates government agencies to maintain the confidentiality of personal records; provides individuals with access to their own records; and ensures that the personal information kept in those records is relevant, necessary, accurate, and secure.[9] However, the Act contains exceptions limiting access to personal information for reasons of criminal law enforcement, defense, national security, foreign policy, and regarding government employment, contracts, and statistics.[10] It also contains exemptions that allow government agencies great freedom in transferring personal information among themselves.[11]

The Privacy Act was based partly on personal data protection principles formulated by an executive committee in 1973. The Act created a new commission that refined and elaborated those principles. The commission's principles provide a well-thought-out framework for evaluating legislative proposals. They are:

The Openness Principle: There shall be no personal-data record-keeping system whose very existence is secret, and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems.

The Individual Access Principle: An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information.

The Individual Participation Principle: An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information.

The Collection Limitation Principle: There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information.

The Use Limitation Principle: There shall be limits on the internal uses of information about an individual within a record-keeping organization.

The Disclosure Limitation Principle: There shall be limits on the external disclosures of information about an individual a record-keeping organization may make.

---

[7] 5 United States Code §552; see also Cate, supra n.1, chapters 4-6, for a useful historical overview of U.S. and European privacy regulation.
[8] See 5 United States Code §552(b)(6),(7)(C).
[9] Id. §552a.
[10] Id. §552a(j),(k).
[11] Id. §552a(b)(1),(3).

The Information Management Principle: A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate.

The Accountability Principle: A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems.[12]

Those principles have found varying expression in U.S., European, Canadian, and international privacy law. In 1980 the Organization for Economic Cooperation and Development (OECD) adopted its influential Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which incorporated a similar list of data protection principles.

In the U.S., government-wide information privacy laws were not accompanied by comprehensive legislation governing businesses or non-profit organizations. Rather, private sector laws have generally addressed specific industries or concerns. Important examples include the Fair Credit Reporting Act of 1970,[13] to protect the accuracy and confidentiality of personal credit information; the Family Education Rights and Privacy Act of 1974,[14] to do the same for educational information; the Cable Communications Policy Act of 1984[15] and the Video Privacy Protection Act of 1988,[16] to protect the confidentiality of personal viewing preferences; the Computer Fraud and Abuse Act of 1984[17] and the Electronic Communications Privacy Act of 1986[18] to protect against computer hackers and viruses; the Telephone Consumer Protection Act of 1991,[19] to regulate telephone solicitations; the Driver's Privacy Protection Act of 1994,[20] to protect the confidentiality of driving records; and the Identity Theft and Assumption Deterrence Act of 1998,[21] to protect against high-tech identity theft and credit card fraud.

C. Other Conceptions of Privacy.

I note that in the U.S., some conceptions of privacy focus on personality and autonomy, including the power to make intimate personal decisions.[22] In the 1960's the U.S. Supreme Court began formulating a Constitutional right to privacy that it has used to invalidate laws prohibiting contraception,[23] abortion,[24] and sodomy.[25]

[12] Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, Appendix 4, Chapter 3 (Washington, 1977).
[13] 15 United States Code §§1681-1681v.
[14] 20 United States Code §1232g.
[15] 47 United States Code §551.
[16] 18 United States Code §2710.
[17] 18 United States Code §1030.
[18] 18 United States Code §2510 et seq.
[19] 47 United States Code §227; see also 47 Code of Federal Regulations §64.1200.
[20] 18 United States Code §§2721-2725.
[21] Public Law 105-318.
[22] See Gormley, supra n.1, at 1337.
[23] *Griswold v. Connecticut,* 381 U.S. 479 (1965).
[24] *Roe v. Wade,* 410 U.S. 113 (1973).

However, Rivki has indicated to me that such personal decision-making powers are not within the scope of our deliberations regarding Israeli privacy law.

A functional classification of privacy interests was formulated in 1972 by a Canadian government task force and later adopted by the Canadian Supreme Court.[26] It classified privacy interests as *personal privacy*, which relates to a person's body; *territorial privacy,* which relates to a person's home and other physical possessions; and *informational privacy*, which relates to personal information.

Many scholars have gone beyond definitions and classifications to discuss the underlying interests and values served by privacy. Alan Westin, David Flaherty, and U.S. legal scholar Ruth Gavison have discussed different aspects or components of privacy, including solitude; anonymity; reserve; intimacy; secrecy; confidentiality; limiting accessibility; minimizing intrusiveness; and maintaining exclusive control of access to private realms.[27]

U.S. legal scholar Fred Cate described privacy as "not an end in itself but rather an instrument for achieving other goals."[28] The values served by privacy include providing individuals with private space to develop ideas and opinions, conduct self-evaluation, and express strong emotions. Privacy also facilitates interpersonal communication, group evaluation, and group decisionmaking.[29]

In sum, conceptions of privacy vary widely, and they develop in tandem with technological and social change. In recent years, the accelerating advance of computer and telecommunications technology has made privacy a subject of increasing discussion and controversy.

III. The Digital Revolution

In recent decades, digital technology has revolutionized the collection, analysis, storage, and transfer of personal information. According to Fred Cate,

[M]ore data than ever before are made available in digital format, which is significant because digital information is easier and less expensive than nondigital data to access, manipulate, and store, especially from disparate, geographically distant locations. And more data are generated in the first place, because of the ease and very low cost of doing so and because of the high value of data in an increasingly information-based society. Data often substitute for what would previously have required a physical transaction or commodity. In electronic banking transactions, for example, no currency changes hands, only data. And recorded data, such as a list of favorite web sites or an automatically generated back-up copy of a document, also make the use of computers easier, more efficient, and more reliable. Finally, our computer

---

[25] *Lawrence v. Texas,* 123 S.Ct. 2472 (2003).
[26] *R. v. Dyment,* [1988] 2 S.C.R. 417.
[27] Westin, supra n.8; Cate, supra n.1, at 21-22, citing David H. Flaherty, Protecting Privacy in Surveillance Societies (1989), at 8, table 1; Ruth Gavison, *Privacy and the Limits of Law,* 89 Yale Law Journal 421, 433 (1980).
[28] Cate, supra n.1, at 23.
[29] Id at 23-28.

technologies and services tend to record what might be characterized as “gratuitous” data, such as the web sites we have visited.
...
Consider this catalog ... of the data that are routinely collected about you:

Your health history, your credit history, your marital history, your educational history, and your employment history.
The times and telephone numbers of every call you make and receive.
The magazines you subscribe to and the books you borrow from the library.
Your travel history. ...
The trail of your cash withdrawals.
All your purchases by credit card or check. In the not-so-distant future, when electronic cash becomes the rule, even the purchases you still make by bills and coins could be logged.
What you eat (no sooner had supermarket scanners gone on line – to speed checkout efficiency – than data began to be tracked for marketing purposes). ...
Your electronic mail and your telephone messages.
Where you go and what you see on the World Wide Web.
...
[T]he Internet is only one tangible example of the explosion of digital information that includes other national and global networks, company computer and telecommunications systems, electronic mail ..., computer bulletin boards, portable telephones, digital facsimile machines, voice mail, nationwide paging services, interactive television, video telephones, and countless other technologies.[30]

As more people use computers at work and at home, data-gathering software can record not only their e-mail and Internet use, but also the content and timing of each individual keystroke. As electronic cash replaces bills and coins – which seems inevitable, given the increasing sophistication of counterfeiters – data-gathering software can record any economic transaction.

As Cate notes, the digital revolution is characterized by global networks and international data transfers, which makes it difficult or impossible for any one nation to regulate privacy. The Internet continuously splits up information transmissions into many small packets and routes the packets through numerous different servers, searching for the quickest path between source and destination at any given moment. (That quality of redundancy also allows the Internet to continue operating even if a part of it is disabled or destroyed.)[31] Determining and exercising legal jurisdiction over Internet transmissions will not be a simple task.

As advances in digital technology have greatly improved data collection, storage, transmission, and processing capabilities, government and corporations have begun to use “data mining” – that is, sophisticated analysis of large quantities of data – to improve the efficiency of their operations. For example, when Internet firms place “cookies” on computer hard drives to collect personal information about users and track their use of the Internet, data mining allows advertising to be targeted

---

[30] Id. at 1-2, 7.
[31] For a good description of the history and structure of the Internet see *American Civil Liberties Union v. Reno,* 929 F. Supp. 824, 830-838 (E.D.Pa. 1996).

specifically to each user.[32] Data mining techniques may use artificial intelligence and statistical techniques to identify patterns and relationships that might otherwise remain hidden.[33] As data mining becomes more common and useful, it is likely to encourage further the drive to collect, store, and process data.

U.S. high-tech scholar Simson Garfinkel argues that the new technology is generally not privacy neutral: "Although it's possible to use technology to protect or enhance privacy, the tendency of technological advances is to do the reverse. It is harder, and frequently more expensive, to build devices and construct services that protect people's privacy than to destroy it."[34] Garfinkel notes that modern data storage facilitates the human tendency to collect and retain information even if it is not for legitimate purposes, and to rely on recorded information even if it is not accurate.[35]

Garfinkel expresses particular concern that the rapid proliferation of medical, psychological, and genetic information may damage lives and careers.[36] Another, more systemic concern is that pervasive recording of personal statements and history may discourage qualified people from seeking office in democratic elections.[37]

While much attention has been paid to the growth of informational databases, Garfinkel, U.S. futurist and science fiction writer David Brin, and other commentators have also catalogued a host of other present-day and near-future surveillance devices that threaten privacy:[38]

Cameras. Governments and private organizations have installed surveillance cameras in an ever-increasing range of locations including roads and intersections, airports, bus and train stations, schools, public parks, prisons, shopping malls, supermarkets, department stores, shops, banks and automated teller machines, convenience stores, parking lots, and offices. Technology continually improves the range, resolution, miniaturization and mobility of cameras. For example, government satellite cameras may now be able to distinguish objects on the ground as small as 10 centimeters across. Brin also predicts the eventual development of tiny, mobile cameras that will be able to fly to designated locations, inflate a gel bubble lens, and collect and relay observations.

---

[32]For a good description of the operation of "cookies" and related devices see *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 500-505 (S.D.N.Y. 2001); Bryan T. McKinney and Dwayne Whitten, *Arkansas Surfers and their Privacy, or Lack Thereof: Does the Common Law Invasion of Privacy Tort Prohibit E-tailers Use of Cookies?*, 24 University of Arkansas at Little Rock Law Review 751, 753-757 (2002); and John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 Alberta Law Review 346, 353-356 (2001).

[33]See Two Crows Corporation, *Introduction to Data Mining and Knowledge Discovery* (1999), available at http://www.twocrows.com/intro-dm.pdf; and, for additional information on data mining, see generally http://www.twocrows.com/, http://www.kdnuggets.com/, http://www.the-data-mine.com/, and http://www.spss.com/.

[34]Simpson Garfinkel, Database Nation (2000) at 258.

[35]Id. at 73-75, 31.

[36]Id. at 129-133, 186-187, 264.

[37]Id. at 88, 258.

[38]See id. at 108 et seq.; David Brin, The Transparent Society (1998); A. Michael Froomkin, *The Death of Privacy*, 52 Stanford Law Review 1461, 1468-1501 (2000); Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003*, Threats to Privacy, available at http://www.privacyinternational.org/survey/phr2003/; and Allen Hunt, Chris Tillery, and Norbert Wild, "Through-the-Wall Surveillance Technologies," Corrections Today, July 2001.

Biometric Identification. Digital technologies enable or improve personal identification through fingerprints, DNA, retinal and iris scans, hand geometry, vein patterns, facial feature recognition, ear shape, and other physical characteristics. Some of those technologies can identify people at a distance, or in a crowd.

Hyper-Visual Devices. Other devices use thermal, infrared, radar, microwave, x-ray, sound, magnetic, or other radiation to penetrate rain, fog, dust and darkness; look though or around the walls of buildings; see with great detail through clothing, luggage, and packages; and eavesdrop on the use of computers.

Audio and Olfactory Devices. Audio surveillance and voice identification may accompany or substitute for video surveillance. Directional microphones can monitor conversations at a distance and through windows and other obstacles. Tiny, camouflaged bugs with internal power supplies can remain active for years. Brin also describes a recently-developed artificial nose – an array of polymer sponges – that detects, classifies and recognizes odors.

Tracking Devices. Cellular telephones, pagers, motor vehicle security devices, electronic toll collectors, radio frequency identification tags, and other devices all allow their users' geographical locations to be tracked with ever-greater accuracy. Governments use location information to coordinate emergency services, recover stolen vehicles, investigate crimes, and enforce traffic and emissions laws, while businesses may use such data to market location-related goods and services.[39]

As technology continues to improve and its uses become more widespread, the implications for privacy will grow.

(I note here that this memorandum does not discuss genetic information issues in detail, because the Ministry of Justice is addressing such issues separately from general privacy legislation. Nonetheless, it is almost certain that as the human genome is progressively decoded during the coming decades, genetic information will become an increasingly important nexus of technology and privacy law.)

In response to technological advances, privacy activists like Garfinkel warn that unless broad protective legislation is enacted, opportunities to protect privacy will be lost. Others disagree, arguing that our inability to predict the effects of technology, coupled with our desire to avoid detrimental unintended consequences, should make our legislative approach cautious, moderate, empirical, and incremental.

James Dewar, a U.S. Rand Corporation scholar, argues that it will be decades before we see the full effects of the information age.[40] While the Internet has become well-known and commonplace, it is still used directly by only a small portion of the

[39] For good discussions of technological and legal developments regarding electronic tracking devices, see generally Matthew Mickle Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 Stanford Law and Policy Review 103 (1998), and Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services,* 10 CommLaw Conspectus 133 (2001).

[40] James A. Dewar, "The Information Age and the Printing Press: Looking Backward to See Ahead," Santa Monica: Rand, 1998, at 3, 5, 12.

population. However, he predicts that by the year 2010 the Internet will become ubiquitous and integral to daily life in the same way that books, telephones, and television sets are today.[41]

Dewar predicts that just as the printing press revolutionized Western culture by introducing "one-to-many" communication, the Internet is doing so by introducing "many-to-many" communication.[42] As the Internet expands and creates new norms, new laws may prove ineffective or harmful. An example of an ineffective law is the ban on software piracy, because software piracy has become socially acceptable: "Whenever there is such profound divergence between the law and social practice, it is not society that adapts."[43] But Dewar is most concerned about legislation that may inadvertently suppress the use and development of the Internet, because countries that do not develop and take advantage of the Internet will fall behind others that do so.[44]

Faced with technologically-inspired privacy concerns on one hand and the European Union's comprehensive regulatory approach on the other (see below), Israeli policymakers may be tempted to enact sweeping reforms. Thus, it may be prudent first to consider some of the costs and disadvantages of privacy, and the virtues of openness and transparency.

IV. The Costs of Privacy

Privacy laws are based on the assumption that privacy is positive, valuable, and deserving of protection. However, privacy laws, and privacy itself, also have costs and disadvantages. Privacy permits concealment, which may facilitate deception and injury.

U.S. legal scholar Amitai Etzioni has argued that disclosure of sensitive personal information is sometimes justified by a greater public good.[45] To illustrate, Etzioni uses the following examples of laws that he supports:

Laws that require notification to a community when a person convicted of child molestation moves in, even though this is a great hardship for the offender who has served his sentence. The extremely high rate of recidivism among child molesters justifies disclosure.

Laws that require AIDS testing of newborn infants, even though the test may also reveal that the mother has AIDS, which may result in stigmatization and discrimination. The low rates of detection among AIDS-infected newborns, and the importance and value of early treatment for such newborns, justifies testing.

Laws that require persons who conceal digital communications with strong encryption technology to provide law enforcement authorities with keys that can unlock the

---

[41]Id. at 7, 9-10.
[42]Id. at 4, 17-20, 24.
[43]Id at 21, quoting John Perry Barlow, "Everything You Know About Intellectual Property is Wrong," *Wired*, Issue 2.03, March 1994.
[44]Dewar, supra n.42, at 25-26, 28-30
[45]Amitai Etzioni, The Limits of Privacy (1999).

encryption. The use of strongly encrypted communications to plan and carry out terrorist and criminal acts, and to prevent prosecution afterwards, justifies law enforcement access.

Laws that require individuals to carry national identification cards or biometric identifiers are justified by the need to apprehend criminals, control immigration, prevent theft and fraud, and collect child support payments.[46]

Note that Etzioni's justifications are based on avoiding severe or unlawful threats to human life, health, or property. He responds to what he sees as Americans' exaggerated distrust of government, but he does not favor limiting privacy for less than urgent reasons. For example, Etzioni opposes the efforts of employers to gather medical or genetic information on their current or prospective employees.[47]

Etzioni's conclusions are subject to dispute, but his analytical approach is shared by most commentators on informational privacy. On the one hand, they evaluate the sensitivity of personal information and accord higher protection to more sensitive information. On the other hand, they weigh policy objectives in opposition to privacy and accord highest protection to safeguarding human life and health, somewhat less protection to comparatively less urgent law enforcement objectives, and still less protection to commercial goals. Then they balance the interests involved and make recommendations.

U.S. federal judge, legal scholar, and free-market advocate Richard Posner has expressed more sweeping reservations about privacy:

Much of the demand for privacy ... concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is ... to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit.[48]

Fred Cate comments in a similar vein:

What parent would not want to know if her child's babysitter had been convicted for child abuse? Similarly, what store owner would not want to know whether a clerk was a kleptomaniac? What patient would not want to know whether his physician had a history of malpractice? What man or woman would not want to know if a potential sexual partner had a sexually transmitted disease? What airline would not want to know if its pilots were subject to epileptic seizures? Yet the interest in not disclosing that information is precisely what privacy protects.
...
Privacy is not an absolute. It is contextual and subjective. It is neither inherently beneficial nor harmful. ... For example, if privacy protects the combination to my safe or the location of a key to my house, it is extraordinarily valuable to me and, in most circumstances, to society more broadly, which shares my interest in avoiding

[46]Id. chapters 1-4.
[47]Id. at 144-146.
[48]Richard A. Posner, *The Right of Privacy*, 12 Georgia Law Review 393 (1978).

theft and other criminal conduct. If privacy allows me to avoid the inconvenience of junk mail, it is somewhat more valuable to me, but less so to others, who benefit from the subsidy paid by bulk mailers and from the ability to target advertisements for products and services. If, however, privacy permits me to avoid paying taxes or obtain employment for which I am not qualified, it may be very valuable to me, but extremely costly to society as a whole.
...
The legal regulation of privacy is significantly influenced by the importance placed by society on the prevention of crime and prosecution of criminals, free expression and an investigatory press, the acquisition and use of property, and a limited role for government involvement in daily life. ... [P]rivacy facilitates the dissemination of false and misleading information, increases the cost of providing products and services, and interferes with meaningful evaluation of students and employees. [It] even conflicts with what may seem to be more mundane interests such as the desire for instant credit, better targeted mass mailings, lower insurance rates, faster service when ordering merchandise by telephone, qualified employees, or special recognition for frequent travelers.[49]

Nonetheless, despite his concerns about the costs of privacy, Cate favors substantial protection of personal information. For example, he recommends that a person who collects non-publicly-available personal information about another person should have to notify the other person what information will be collected, how it will be used and disseminated, how long it will be retained, and whether there is a legal obligation to provide the information; if there is no legal obligation, the person collecting the information should have to obtain the other person's consent, either explicit or implicit, depending on the information; and additional consent should be required if the person collecting the information wishes to change the conditions of the notice.[50]

Other thinkers and commentators are more skeptical about the utility of privacy regulations.

In his influential dystopian science fiction novel The Shockwave Rider (1975), British author John Brunner described a global society structured around a universal government-controlled computer information network. The government and large corporations control enormous amounts of personal and confidential data, while private citizens have much more restricted access. The novel's hero is a computer hacker who recognizes that there is no way to prevent powerful interests from obtaining and exploiting information. His solution is to level the playing field by introducing a computer virus into the network that makes all information available to all citizens.

Brunner's novel is often cited as an early prediction of the Internet, and his use of the term "worm" to describe a self-replicating, self-propagating computer program was later adopted by the computer industry. His view that government and powerful corporations will always have access to personal data, and that therefore the solution is to increase openness rather than privacy, has been influential.

---

[49] Cate, supra n.1, at 29, 31, 100, 102.
[50] Id. at 112-119.

David Brin also argues that in a transparent society, the right to keep secrets "will not enhance the average person's freedom for one simple reason: *the rich and powerful are sure to be far, far better at exploiting that right than little people ever will be, any time, any place.* ... If the tycoon and bureaucrat have it in their power to tap a key and get my location or my dossier, then I want to be able at least to find out that they are looking, and possibly to look right back at them."[51] Brin notes that "no other populace has ever had so much known about them, both in groups and as individuals", but because people are unaware of who has their personal information and how it is used, they maintain an illusion of privacy rather than real privacy.[52]

Brin does support protecting the secrecy of sensitive information in sensitive areas such as national security; medical records; relationships with therapists, attorneys, and clergy; and professionals' consultative meetings.[53] But regarding less sensitive information he argues that "the public's concern for privacy is like the River Platte, a mile wide but only an inch deep."[54] Brin recommends that government, instead of wasting its limited resources fruitlessly trying to regulate exploding information flows, should focus on prohibiting misuse of information:

[C]ommon sense shows that it matters less what a person knows than what she or he does with the knowledge.
...
When you choose to give strangers your telephone number, it becomes a password, offering them the power to intrude on you at home. But what about when you call out for a pizza? Often nowadays ... the restaurant begins by asking your phone number, to check their computer records ... [so] you won't have to repeat lengthy delivery instructions. ... [T]he clerk obligingly asks, "Do you want pineapple and anchovies, like last time?"

If I order from a gift catalog, do they want my phone number because their filing system needs it to find me? Or because they want to have their autodialer robot call and breathlessly explain their latest sale, every week, during dinnertime, for the rest of my life? (A clear case for legal restraint of information flow!)[55]

Brin optimistically favors the free flow of information, not only because it holds powerful institutions accountable, but also because it powerfully contributes to social, economic, scientific and artistic progress, and because it promotes tolerance. On the latter point, he quotes U.S. cartoonist-humorist Scott Adams – "In the future, new technology will allow the police to solve 100 percent of all crimes. The bad news is that we'll realize 100 percent of the population are criminals, including the police" – then U.S. Internet policy expert Esther Dyson – "we may all become tolerant if everyone's flaws are more visible" – and concludes by asking, "might we learn to 'chill out' when everyone realizes that people who live in glass houses are unwise to cast stones?"[56]

---

[51]Brin, supra n.40, at 201, 242 (emphasis in original).
[52]Id. at 157, 9-14.
[53]Id. at 64-65, 210.
[54]Id. at 153; see also Jeffrey Rosen, The Unwanted Gaze (2000) at 197.
[55]Brin, supra n.40, at 244, 239.
[56]Id. at 23, 331.

Does transparency promote tolerance? The human impulse to hide sensitive information is based on a reflexive fear that disclosure will bring harm, not benefit. David Flaherty notes that

I have rarely met anyone who can satisfy me that they do not [value personal privacy]. People sometimes say to me, "I really don't worry about my privacy, because what do I have to hide?" But one has only to start asking questions about "How much money do you have in your bank account?", "Have you ever had psychiatric care?", or "Have you ever had an abortion?", and people quickly discover, "Well, I do have some sense of privacy in the form of a fair amount of information about myself that I prefer to keep under my control."[57]

The complicated truth is that regarding sensitive information, both privacy and transparency have benefits.

For example, psychotherapy, while often beneficial, is sometimes stigmatized. If a person's therapeutic history is disclosed, he may suffer negative consequences in employment and personal relationships. However, as the therapeutic experiences of many people are disclosed, it reduces the stigma of therapy and thus helps other people overcome their hesitation and begin to benefit from therapy. This is especially true if information is identifiable. People who could benefit from therapy are unlikely to be influenced by dry statistics, but if they have concrete knowledge of the specific therapeutic experiences of people who are known to them, it could encourage them to seek therapy and help them to identify suitable treatments and competent therapists.

Similarly, shame and fear have prevented many victims of rape and domestic abuse from disclosing their identities and experiences. But as more people have stepped forward and told their stories, awareness has grown, which has encouraged still more people to address the problem in their own lives, and in society at large.

A third, very controversial example of the conflict between privacy and transparency is the practice of homosexual "outing." Some gay and lesbian activists argue that disclosing the homosexual orientation of public figures, even against their will, is justified by the need to advance social acceptance and legal progress for homosexuals. In 1996, while the U.S. Congress was debating a bill to prevent the legalization of homosexual marriage, activists publicized the homosexuality of several Congressmen who supported the bill.[58] For similar reasons, British activists "outed" ten Anglican bishops in 1994.[59]

However, the story of Oliver Sipple, which is well-known within the U.S. gay and lesbian community, sounds a more cautionary note about "outing." In 1975, Sipple, a troubled Vietnam veteran, prevented a would-be assassin from firing at President Ford. In the ensuing publicity Sipple's homosexuality was disclosed by the media.

---

[57]Flaherty, supra n.7, at 220.

[58]See Michelangelo Signorile, "Outing's Triumphant Return," *OUT,* December 1996/January 1997; J. Jennings Moss, "On the Record," *The Advocate,* September 3, 1996; "Lesbian Notions," *Seattle Gay News Online*, December 24, 1999.

[59]See Peter Tatchell, "Outing is a Catalyst for Social Change" (1995), at http://www.tatchell.freeserve.co.uk/outing/catalyst.htm; and http://www.outrage.org.uk/gall96.htm.

Sipple became estranged from his family and suffered from increased emotional difficulties and alcoholism until his death in 1989.[60]

Sipple's story is among those cited by U.S. legal scholar Jeffrey Rosen, who argues that privacy protects individuals from being unfairly misjudged. Rosen's writing focuses on public figures and political conflicts, but his observations have some application to ordinary lives as well. Rosen argues that

Privacy prevents us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.
...
[W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences.
...
[A]s intimate information about our lives is increasingly recorded, archived, and made hard to delete, there is a growing danger that a part of our identity will be confused with the whole of our identity.
...
[P]rurient information is so luridly interesting that, when widely publicized, it crowds out all other topics of public discussion, making it difficult to think or talk about anything else.[61]

Despite Rosen's concerns, Brin is probably correct when he predicts that a more transparent society is inevitable, and that it may prove beneficial in the long run. Nonetheless, governments should exercise their powers to prevent abusive violations of privacy. The most comprehensive, systematic, and influential legislation protecting personal information privacy is that of the European Union, which I will discuss next.

V. **European Union Data Protection Laws**

A. Background.

European privacy law has been strongly influenced by German and French history and law. In part because Nazi Germany's crimes were facilitated by totalitarian control of personal information, West Germany legislated very strict privacy laws, a tendency that was strengthened by its 1989 reunification with the formerly Communist totalitarian police state of East Germany.[62] France also adopted strict

[60]See Beth Ann Krier, "Whose Sex Secret Is It?", *Los Angeles Times,* May 22, 1990; "The Oliver Sipple Page," at http://www.lambda.net/~maximum/sipple.html.

[61]Rosen, supra n.56, at 8-10, 142.

[62]See Alexandra Samuel, "Privacy and Security Turn from Friends to Enemies," *Vancouver Sun,* November 9, 2001; Solveig Singleton, "Privacy and Human Rights: Comparing the United States to Europe," Cato Institute, December 1, 1999; Rita M. Walczuch and Lizette Steeghs, "Implications of the New EU Directive on Data Protection on Multinational Corporations," *Information Technology and People,* Vol. 14(2), June 2001, at 3.

privacy laws, and other European nations, responding in part to German and French influence, have adopted broad privacy laws of their own.[63]

The Charter of Fundamental Rights of the European Union incorporates privacy rights in its second chapter, "Freedoms", in Articles 7 and 8:

Article 7
Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.[64]

B. The Data Protection Directive.

The EU's 1995 Data Protection Directive,[65] which is based mainly on German and French law,[66] is the EU's foundational legislation for protecting personal data. The Directive requires EU member states to enact legislation implementing its terms and establish supervisory bodies to monitor compliance and enforce the laws.

The Directive employs a few key terms that assist in understanding its provisions:

"personal data" is any information relating to an identified or identifiable natural person (a "data subject");
"processing" is any operation performed on personal data, including collection, recording, combination, modification, organization, storage, retrieval, use, disclosure, blocking, or destruction;
a "controller" is a natural person or organization that determines how personal data will be processed; and

---

[63]See Marsha Cope Huie et al., *The Right to Privacy in Personal Data: the EU Prods the U.S. and Controversy Continues*, 9 Tulsa Journal of Comparative & International Law 391, 456-458 (2002).
[64]Charter of Fundamental Rights of the European Union (2000/C 364/01), Articles 7-8.
[65]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[66]See Walczuch, supra n.64, at 7, 13.

the “supervisory authority” is the public authority within an EU member state that is responsible for monitoring the implementation of its personal data protection laws.[67]

The Directive grants broad rights to data subjects but also creates broad exceptions. Some commentators argue that the exceptions may swallow the rules.[68]

Purposes of Processing. Under the Directive, personal data may be collected only for specified, legitimate purposes. The data may not be processed for other purposes, unless those purposes are historical, statistical or scientific. Only relevant data may be collected and processed. Data must either be kept accurate or erased. After the original purposes of processing have expired, the data may not be retained in a form that identifies the data subject.[69]

Consent of Data Subject. A controller may process personal data only with the data subject’s unambiguous consent. However, consent is not required if the processing is necessary to perform a contract for the data subject; to protect the data subject’s vital interests; to comply with a legal obligation; to perform a task in the public interest or in the exercise of official authority; or for other legitimate interests of the controller or third parties.[70]

When a controller relies on the “public interest,” “official authority,” or “legitimate interests” exceptions, the data subject may object to the processing if he has compelling, legitimate grounds. The data subject may also object to processing of his personal data without consent for direct marketing purposes.[71]

Notice to Data Subject. When personal data is collected from a data subject, the controller must identify itself and inform the data subject of the purposes of the processing.[72] When personal data is collected from other sources, the controller must notify the data subject before recording the data or disclosing it to third parties, unless the processing is for statistical, historical or scientific purposes.[73]

Access for Data Subject. When a data subject inquires, a controller must confirm whether it is processing personal data relating to him. If so, the controller must describe the data, the purposes of processing, and the processing itself. The controller must also identify third parties to whom the data is disclosed. The data subject is entitled to rectify incorrect data, and the controller must provide notice of such corrections to third parties to whom it disclosed the incorrect data, unless such notice would require disproportionate effort. The data subject is also entitled to obtain erasure or blocking of data to prevent unlawful processing.[74]

---

[67]EU Directive 95/46/EC, supra n.67, Articles 2, 28(1).
[68]See Stephen A. Oxman, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?*, 24 Boston College International & Comparative Law Review 191 (2000).
[69]EU Directive 95/46/EC, supra n.67, Article 6.
[70]Id. Article 7.
[71]Id. Article 14.
[72]Id. Article 10.
[73]Id. Article 11.
[74]Id. Article 12.

Significant Decisions. The data subject may not be subjected to significant decisions based solely on automated processing of data that evaluates personal areas like job performance, creditworthiness, reliability, and conduct. However, there are exceptions where processing is necessary to perform a contract with the data subject, or is otherwise authorized by law.[75]

Confidentiality and Security. Controllers must take reasonable steps to safeguard the confidentiality and security of personal data.[76]

Sensitive Data. The Directive prohibits the processing of personal data revealing race, ethnicity, political opinions, religious or philosophical beliefs, health, or sex life. (The Directive also suggests that only government authorities should process criminal records.) However, exceptions allow controllers to process sensitive personal data under the following conditions:

if the data subject explicitly consents;
if the information is already publicly available;
to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent;
for preventive medicine, medical diagnosis and treatment, and management of health care services;
to carry out employment-related rights and obligations;
to establish, exercise, or defend legal claims;
when a non-profit political, philosophical, religious, or trade union organization processes data on its members or on other persons with whom it has regular contact; or
for other reasons that member states decide are in the public interest.[77]

Supervisory Authorities. The supervisory authorities are independent administrative agencies that are empowered to hear claims of privacy violations, conduct investigations, make orders, and pursue legal proceedings. They also have advisory roles on policy.[78]

A controller must notify its member state's supervisory authority before processing personal data, unless the processing is unlikely to injure the rights and freedoms of data subjects. The supervisory authority must keep a register of processing operations and insure that they are publicized. When proposed processing operations present specific risks to data subjects, the supervisory authority must evaluate the proposed operations and decide if they may proceed.[79]

---

[75] Id. Article 18.
[76] Id. Articles 16-17.
[77] Id. Article 8; see also the EU regulation applying the Directive's requirements to EU government bodies, Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
[78] EU Directive 95/46/EC, supra n.67, Article 28.
[79] Id. Articles 18-21.

Judicial Remedies. Data subjects claiming privacy violations may bring suit against controllers in court and receive compensation. Member states must adopt appropriate sanctions for violations.[80]

Broad Exemptions. In addition to the exceptions described above, the Directive has several broad exemptions that greatly limit its applicability.

First, the Directive does not apply to processing operations concerning the European Union's foreign and security policy; immigration and asylum policy; judicial cooperation; customs cooperation; police cooperation against terrorism, drug-trafficking and other serious international crimes; programs to combat drug addition; and programs to combat international fraud.[81]

Second, EU member states may exempt themselves from the Directive's requirements in matters regarding national security; defense; public security; enforcement of criminal law or professional ethics; important economic or financial interests, including monetary, budgetary, and taxation matters; the protection of (unspecified) rights and freedoms; scientific research; and statistical operations.[82]

Third, EU member states must provide exemptions from the Directive's requirements to ensure freedom of expression for journalism, art, and literature.[83]

In sum, the Directive generally does not apply to government, news media, and the arts. Broad exemptions are also provided for scientific, historical, and statistical activities. Non-profit organizations, health care providers, and employers are exempt from some requirements regarding sensitive personal data. And there are exceptions that apply to contracts with data subjects and other legal obligations.

On the other hand, businesses that are non-journalistic and non-artistic, and that wish to use personal data for marketing, receive no exemptions. In fact, there are special restrictions applicable to direct marketing.

Thus, ironically, although European privacy law originated from reactions to the abuses of totalitarian governments, the EU data protection law is now directed primarily at private enterprise.[84]

Data Transfer Restrictions. The Directive prohibits the transfer of personal data to controllers in non-EU countries that do not ensure "an adequate level of protection."[85] So far the European Commission has determined that four nations – Switzerland, Hungary, Canada, and most recently Argentina – provide an adequate level of protection.[86]

[80]Id. Articles 22-24.
[81]Id. Article 3(2); see also Treaty on European Union (1992) Articles V and VI.
[82]EU Directive 95/46/EC, supra n.67, Article 13.
[83]Id. Article 9.
[84]See Singleton, supra n.64.
[85]EU Directive 95/46/EC, supra n.67, Article 25.
[86]See European Commission Decisions 2000/518/EC of 26 July 2000 (Switzerland); 2000/519/EC of 26 July 2000 (Hungary); 2002/2/EC of 20 December 2001 (Canada); and C(2003)1731 of 30 June 2003 (Argentina).

Of course, the EU has not severed its trade relations with the rest of the world. The Directive provides exceptions that permit data transfers to non-approved countries under the following circumstances:

with the consent of the data subject;
to perform a contract for the data subject;
to protect the vital interests of the data subject;
with data taken from a public register;
in connection with legal claims; or
for important public interests.[87]

In addition, EU member states may permit transfers to non-approved countries where controllers adopt adequate safeguards, such as appropriate contract clauses, and the EU is informed of the exceptions.[88] In 2001 the EU issued standard contract clauses that comply with the Directive and may be used as a model or guide by controllers.[89] The standard clauses generally incorporate the principles of the Directive, provide data subjects with legal forums and remedies for abuses, and subject non-EU parties to the jurisdiction and oversight of EU supervisory authorities and controllers.[90]

It is also worth noting that in 2000 the EU approved safe harbor provisions negotiated with the U.S. that allow personal data transfers to U.S. organizations.[91] However, it is unlikely that other nations will be able to rely on similar provisions, because the safe harbor provisions' combination of self-regulation and government oversight is adapted specifically to U.S. law,[92] and because, realistically, it reflects U.S. bargaining power more than U.S. compliance with EU law.[93] In 2002 the EU released a working paper concluding that the formal elements of the safe harbor arrangement are in place, but that concerns remain regarding self-regulation, transparency, and enforcement.[94]

Implementation of Directive. The Directive directed all member states to enact laws implementing the Directive by October 25, 1998. Most member states did not meet the deadline, and the EU took a number of formal enforcement steps against non-compliant member states, culminating in court action against five member states in

---

[87]EU Directive 95/46/EC, supra n.67, Article 26(1).
[88]Id. Article 26(2), (3).
[89]2001/497/EC: European Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.
[90]Id. Annex, including Appendices 1 & 2.
[91]2000/520/EC: European Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
[92]See id. Annex I.
[93]See Steven R. Salbu, *The European Union Data Privacy Directive and International Relations,* 35 Vanderbilt Journal of Transnational Law 655, 678-684 (2002).
[94]The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (February 14, 2002).

January of 2000.[95] At this time almost all member states have enacted compliant data protection legislation[96] and created supervisory authorities.[97]

The laws enacted by member states generally follow the principles of the Directive but also incorporate national variations. While a detailed description of each law is beyond the scope of this memorandum, it is worth briefly describing some variations that have been adopted by a number of member states, since they may have more general applicability. Member states have adopted the following variations:

expanding the list of government activities that are exempt from data protection restrictions to include social welfare and judicial activities;
allowing governments to process racial information, even though it is sensitive, in order to address racial inequalities;
providing insurance companies with special access to personal data so that they can provide insurance and combat fraud;
providing businesses with exceptions to some disclosure requirements so that they can protect their trade secrets;
providing special protection for data subjects regarding their credit information and personal identification numbers;
allowing data subjects to block direct marketing contacts by putting their names on national lists;
preventing controllers from demanding certain kinds of personal data from data subjects as a condition for employment or contracts for services;
requiring controllers to notify data subjects of the sources from which they received personal data;
requiring controllers to notify data subjects of the decision criteria they used to make certain decisions based on personal data; and
reducing the level of data protection accorded to basic, publicly available information such as a data subject's name, address, sex, date of birth, telephone and fax numbers, e-mail address, occupational title and position, and academic degrees.[98]

---

[95] See EU press release IP/00/10, Brussels, 11 January 2000.

[96] The EU website records current status of member state legislation and provides links to text at http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm.

[97] For links to both EU and non-EU national supervisory authorities, see the EU website at http://europa.eu.int/comm/internal_market/privacy/links_en.htm. Another web site with links to both supervisory authorities and legislation is http://pages.britishlibrary.net/rwong/DP%20Authorities.htm.

[98] See Act on Processing of Personal Data (Act No. 429, 31 May 2000) (Denmark) §§11 (identification numbers), 12 (basic information), 19-26 (credit information), 36(2) (direct marketing); Personal Data Act (523/1999, 22 April 1999) (Finland) §§12(11) (insurance), 26(1) (data sources), 26(2) (credit information); Federal Data Protection Act (18 May 2001) (Germany) §§28(3)(3) (basic information), 34(1)(3) (trade secrets); Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (9 April 1997) (Greece) Articles 7(2)(v)(cc) (social welfare), 8(3) (identification numbers), 13(3) (direct marketing); Data Protection (Amendment) Act 2003 (10 April 2003) (Ireland) §5, adding §4(13) to Data Protection Act 1988 (employer data requests); Personal Data Protection Act (2000/302, 6 July 2000) (Netherlands) Articles 2(2)(e) (judicial activities), 18 (racial inequality), 21(b) (insurance), 42(4) (decision criteria); Organic Law 15/1999 of 13 December on the Protection of Personal Data (BOE 298) (Spain) Articles 11(2)(d) (judicial activities), 13(3) (decision criteria), Second additional provision (basic information), Sixth additional provision (insurance); Personal Data Act (1998:204, 29 April 1998) (Sweden) §22 (identification numbers); Data Protection Act 1998 (16 July 1998) (United Kingdom) §§8(5) (trade secrets), 30 (social welfare), 56 (employer data requests), Schedule 3 §9 (racial inequality); EU Regulation (EC) No. 45/2001, supra n.79, Articles 12(1)(f)(iv) (data sources), 13(d) (decision criteria), 46(c) (judicial activities).

EU Report on Implementation of Directive. Last May the EU released its first report evaluating the Directive's implementation thus far.[99] The report noted that implementation has been slower than anticipated due to resistance from member states and business interests.[100] A number of member states criticized parts of the Directive and advocated modifying it before implementation, but the EU responded by insisting on implementation first, to be followed by modifications if necessary.[101] In the report, the EU criticized member states' legislation for diverging from the Directive's requirements and threatened to take measures to enforce greater conformity if necessary.[102]

The report also concluded that public awareness and concern regarding personal data protection remain low; enforcement efforts by supervisory authorities are lax or underfunded; the risk of punishment for violations seems low; and that therefore, compliance by data controllers is "very patchy."[103]

Commentary on EU Directive. The Directive's implementation is still at an early stage, so present-day commentary assessing its strengths and weaknesses is inherently speculative. Nonetheless, it is worth briefly reviewing some typical views expressed by commentators.

Some commentators are concerned that the Directive will stifle economic growth and progress. They argue that the Directive does not solve specific, existing, identifiable problems. Rather, it creates a preemptive, bureaucratic, discretionary regime whose restrictive yet unpredictable implementation will discourage and hinder the development of innovative economic activity. Restricting data flow may hurt many new service industries whose business relies on information collection and dissemination. And restricting data-based marketing may increase the cost of marketing, thus driving up the prices of goods and services and also stifling competition by making it much more difficult for new or small businesses to develop a customer base.[104]

Other commentators support the Directive's philosophy but worry that its numerous, broad exemptions may neutralize its effectiveness,[105] or that its sweeping provisions may be impossible to enforce.

Still others are more optimistic, arguing that the Directive does not interfere with business; rather, it merely requires companies to provide more information and options to consumers. In fact, data protection may assist business development by allowing consumers to proceed with more confidence.[106]

C. Electronic Communications.

[99]Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC),* COM(2003) 265, 15 May 2003.
[100]Id. at 1 (including n.1), 3, 10
[101]Id. at 7-8, 17.
[102]Id. at 10-12, 24.
[103]Id. at 8, 12-13, 15, 19, 26.
[104]See Lucas Bergkamp, "EU Data Protection Policy," *Computer Law & Security Report,* v. 18, no. 1, p. 31 (2002); Singleton, supra n.64; Walczuch, supra n.64, at 11.
[105]Oxman, supra n.70.
[106]Huie, supra n.65, at 401; and see also Walczuch, supra n.64, at 21.

Last year the EU issued a directive applying the principles of Directive 95/46/EC to electronic communications.[107] The directive addresses the use of modern technologies like the Internet, the World Wide Web, and "cookies"; e-mail and "spam"; telephones, caller/receiver identification, and automatic calling machines; mobile telephones and location finders; and faxes. Member states are directed to enact legislation complying with the directive by 31 October 2003;[108] however, if past performance is a reliable guide, implementation is likely to be delayed.

Under the directive, controllers may process personal data in order to provide goods and services; bill customers; detect errors and technical failures; detect fraud; settle disputes; assist in emergencies; stop malicious or nuisance communications; and, in some cases, to market related goods and services. However, automated and electronic marketing is generally forbidden without the data subject's consent, and controllers must erase data when it is no longer relevant. Like the 1995 directive, the 2002 directive is intended to protect the data subject's rights to receive notice, grant or withhold consent, and maintain confidentiality.

The 2002 directive replaced and substantially updated a 1997 directive[109] on the same subject. In response to the terrorist attacks of September 11, 2001, the 2002 Directive increased government powers to use personal data regarding electronic communications for anti-terrorist purposes.

The descriptive summaries provided thus far show that the U.S. and the EU differ substantially in their approaches to some privacy issues. Before detailing my specific recommendations, I will briefly compare different views and circumstances that may assist Israel in understanding and benefiting from comparative privacy law.

VI. The United States, the European Union, and Other Sources of Law

According to the Dutch commentator Rita Walczuch:

"A concrete comparison shows the following differences between [the] EU and [the] US when approaching data protection:

Americans:

are more trusting of the private sector and the market (not the government);

believe in the power of the mass media to check possible abuses in the private sector;

[107] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; see also EU Regulation (EC) No. 45/2001, supra n.79, Chapter IV.

[108] EU Directive 2002/58/EC, supra n.109, Article 17(1).

[109] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

are inclined to think that technologies can contribute to the solutions of problems created by technologies;

are fairly inclined to engage in a cost-benefit analysis of regulatory alternatives;

are more inclined to adopt reactive rather than proactive regulations; [and]

are more prone to adopt regulations that give consumers information about private sector practices in order to enable them to exercise their market power to shop for firms with good policies.

Europeans:

tend to think of self-regulation as being equal to no regulation;

are inclined to overprotect rather than underprotect; and

craft relatively narrow exceptions to broadly applicable rules.

Furthermore, there is a big difference between the two cultures when conceiving the nature of people's interests in data about themselves. In the European Directives, data protection belongs to the 'fundamental rights' of citizens. In contrast to that, Americans favor a free flow of information, which is embodied in the First Amendment [to the U.S. Constitution]."[110]

Both the American and European approaches have strengths and weaknesses. Americans reason that because consumers have many goods and services from which to choose, private firms have a strong interest in satisfying and not offending them. For example, a study of American and European web sites found that although Europe has tougher and more comprehensive data protection laws than the U.S., the American web sites had much better privacy policies than the European websites.[111] While Americans' trust is not blind – they also rely on a vigorous press to disclose abuses, and sometimes on legal action – they generally fear private enterprise less than they fear the government. Government bureaucracies, they reason, have immense power – power to regulate, prohibit, tax, fine, confiscate, imprison, and kill – and bureaucrats often don't care whom they offend.

However, the American approach sometimes reacts very slowly when entrepreneurs don't care whom they offend. For example, the U.S. Federal Trade Commission recently opened its "Do Not Call Registry" allowing consumers to place their telephone numbers on a national registry that blocks telemarketing calls. In the first two months almost fifty million people subscribed.[112] That energetic response is an indicator of the time wasted, and the aggravation caused, by unrestricted telemarketing over the years.

[110]Walczuch, supra n.64, at 4-5 (citations omitted).
[111]See MacDonnell, supra n.34, at 365-366.
[112]See Federal Trade Commission press releases, "Do Not Call Registry Tops 30 Million Phone Numbers," August 6, 2003, and "Do Not Call Registry Jumps to 48.4 Million," September 2, 2003.

Unsolicited commercial e-mail – "spam" – also wastes time and causes aggravation. In addition, the enormous and growing volume of spam is a significant financial drain on Internet service providers, and it slows down Internet traffic. Yet although the problem has been building for years, the U.S. has yet to enact an anti-spam law.[113]

The U.S. approach sometimes fails to address problems until they reach crisis proportions. On the other hand, it also helps to make the U.S. the most economically, technologically, and culturally dynamic nation on Earth. By way of contrast, Germany and France favor pro-active, comprehensive, bureaucratic regulation, but some commentators argue that such high levels of regulation contribute to economic stagnation in both countries. It remains to be seen whether the EU data protection regime will encourage multinational corporations to relocate from Europe to the U.S., Asia, and elsewhere.

In recent years the contrast between the EU and the U.S. has grown sharper. The EU is moving firmly and steadily to impose uniform data protection regulations on EU member states and, indirectly, on other nations to whom those member states transfer personal data – in other words, on the whole world. On the other hand, in the two years since the terrorist attacks of September 11, 2001, the U.S. has led a worldwide trend to subordinate privacy concerns to security considerations.[114]

The EU's comprehensive approach may create difficulties for other countries. As noted above, the EU's 1995 Directive forbids member states from transferring personal data to countries that do not have adequate data protection. Adequate data protection includes a commitment not to transfer personal data to countries without adequate data protection. In other words, a country that wishes to trade freely with the EU may have to forgo trading with other countries, including the U.S. Some U.S. officials have characterized the EU's transfer restrictions as a potential barrier to free trade, criticized the EU's standard contract clauses as unduly burdensome, and even expressed doubts about continuing the implementation of the EU-U.S. safe harbor agreement.[115] Thus, disagreements between the U.S. and the EU on data protection issues will probably have diplomatic and economic consequences for other countries.

However, the EU standard contract clauses do allow other countries to address data protection issues on a transaction-by-transaction basis, thus avoiding difficult choices between U.S. and EU markets. And it may even be possible for countries to maintain privileged trade relations with both the EU and the U.S., although only time will tell. Canada, which maintains excellent trade relations with the U.S. and is also one of the few nations whose data protection laws have been approved by the EU, may provide an instructive example for other countries.

---

[113]See Christopher Caldwell, "You've Got Spam," *The Weekly Standard*, June 16, 2003; Howard Beales, Director, Bureau of Consumer Protection, Federal Trade Commission, "Unsolicited Commercial Email," testimony before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, Subcommittee on Telecommunications and the Internet, U.S. House of Representatives, Washington, D.C., July 9, 2003.

[114]For an excellent discussion of differences, interactions and potential conflicts between the US and EU approaches, see Salbu, supra n. 95, at 685-695.

[115]See Huie, supra n.65, at 395-402, 461-462; *Privacy and Human Rights 2003*, supra n.40, Overview, Transborder Data Flows and Data Havens.

As an aside, I note that Canada has well-developed privacy laws, on both the federal and provincial levels.[116] Quebec, in particular, has been developing detailed privacy laws since the 1970's.[117] Canada has broad privacy laws that are overseen by independent commissioners, which resembles the European model in some respects. However, like the U.S., Canada focuses primarily on regulating and providing access to personal data held by government agencies, while relying to some extent on self-regulation in the private sector.[118] While a detailed analysis of Canadian law is beyond the scope of this memorandum, I have found it to be a rich source of comparative law, on a par with the U.S. and Europe. Australia, too, is an excellent source of comparative privacy law.[119]

The U.S. is probably the most dynamic legal laboratory in the world. Federal law interacts with fifty state legal systems; statutes and regulations are interpreted and supplemented by judges at common law; and a politically active and litigious culture continually advances the law-making process. When they are on point, U.S. law and scholarship are always worth consulting.

However, the U.S. approach to privacy law has not been as systematic as that of Europe, Canada or Australia. The European approach, which attempts to analyze and regulate privacy matters in a more unified fashion, generates theoretical insights and practical solutions not found in U.S. law.

When Israeli policymakers wish to consult foreign privacy laws, a survey of U.S., European, and perhaps Canadian and Australian law will almost always provide an instructive and fairly comprehensive array of policy considerations and regulatory approaches. If time is limited, research need not go far beyond those jurisdictions.

Based on my own research, I do not recommend that Israel adopt the privacy laws of any one country or region. Rather, I recommend the adoption from each jurisdiction of those measures that are likely to work best in Israel.

[116] The primary Canadian federal privacy laws are the Privacy Act (R.S. 1985, c. P-21), and the Personal Information Protection and Electronic Documents Act (2000, c. 5). The Privacy Commissioner of Canada maintains a website at http://www.privcom.gc.ca/. Links to provincial laws and privacy commissions may be found at http://canada.justice.gc.ca/en/ps/atip/provte.html.

[117] See historical summary at http://www.cai.gouv.qc.ca/eng/cai_en/cai_his_en.htm. Quebec's primary privacy laws are L.R.Q., chapter A-2.1, An Act respecting access to documents held by public bodies and the protection of personal information, and L.R.Q., chapter P-39.1, An Act respecting the protection of personal information in the private sector.

[118] *Privacy and Human Rights 2003*, supra n.40, Overview, Comprehensive Laws.

[119] See website of the Australian Privacy Commissioner at http://www.privacy.gov.au/, with links to federal and state privacy laws and commissions.