

29/8/2022

המטרות והעקרונות לתיקון פקודת הסטטיסטיקה – הערות המכון הישראלי למדיניות טכנולוגיה

אנו מתכבדות להגיש את התייחסות המכון הישראלי למדיניות טכנולוגיה (להלן – **המכון**), ביחס לבקשת הלשכה המרכזית לסטטיסטיקה (להלן – **הלשכה**) לקבלת הערות מאת הציבור בנושא "המטרות והעקרונות לתיקון פקודת הסטטיסטיקה" כפי שפורטו על ידי הלשכה לצורך קבלת הערות הציבור, והועברו לידי המכון בתחילת חודש אוגוסט.

המכון הישראלי למדיניות טכנולוגיה

המכון הישראלי למדיניות טכנולוגיה הוא מכון מדיניות וצוות חשיבה (Think Tank) הפועל לקידום דיוני מדיניות בסוגיות חברתיות, אתיות ומשפטיות מורכבות בעידן הטכנולוגי. המכון מהווה פלטפורמה לכינוס קהילות וגיבוש שיח בין בעלי עניין שונים ובכלל זה גופי ממשל, תעשייה, אקדמיה וחברה אזרחית, לצורך גיבוש ניירות עמדה, מאמרים, וכללי התנהגות מוסכמים (Best Practices) בתחומי מדיניות טכנולוגיה, וקידום פרקטיקות אתיות מעשיות תוך קידום חדשנות.

המכון הוא שלוחה ישראלית של הפורום לעתיד הפרטיות בארה"ב Future of Privacy Forum, מכון מחקר אמריקאי בעל שלוחות נוספות באירופה ובמזרח אסיה, בתחום מדיניות הפרטיות וזכויות אדם. **הפורום והמכון** **נתמכים** על ידי מגוון רחב של חברות מהעולם ומישראל, העוסקות בתחומים שונים, כולל טכנולוגיה, אינטרנט, תקשורת, פיננסים, בריאות, קמעונאות, ועוד. בנוסף לחברות מן המגזר הפרטי, נתמך הפורום בידי קרנות מחקר ממשלתיות ופרטיות. לפורום והמכון ועדות מייצעות הכוללות נציגי חברה אזרחית ואקדמיה כמו גם נציגי תעשייה. למידע נוסף אודות המכון, מומחיו ותומכיו ראו אתר המכון **בא**.

המידע הכלול במסמך זה מייצג את עמדות חוקרות המכון ואינו מייצג את עמדות מי מתומכי המכון או הפורום. המסמך נערך בסיועה של עו"ד ליאור גולדווסר, המתמחה במכון, שסקרה את המצב הקיים במדינות שונות.

הנגשת מידע ופרטיות

המגמה אליה מבקשת הלשכה להוביל את תיקון החקיקה כמשתקף מהעקרונות שפורסמו, והעובדה שהלשכה ביקשה להיוועץ עם הציבור בשלב מקדים, טרם גיבוש המדיניות וניסוחה כחקיקה – מבורך וחשוב. הניסיון למקסם את השימוש במידע המצוי בידי הלשכה ולהנגיש אותו במידת האפשר, תוך שמירה על הפרטיות, היא המגמה אליה צריכה לחתור החקיקה החדשה. האיומים כמו גם הפתרונות בתחום זה מורכבים ומשתכללים כל הזמן. לפיכך, חשוב להסדיר את המסגרת הנורמטיבית הקובעת את העקרונות ואת אבני היסוד אשר יאפשרו ביצוע איזון כאמור בחקיקה ראשית, ולעגן את הסדרת הפתרון הקונקרטי בהסדר משני המאסדר ומשקף לציבור את דרך הנגשת הנתונים והתממתם, אך גמיש יותר לשינויים. כמו כן על הלשכה לקבוע כי המתודות והכללים שייקבעו ייבחנו אחת לתקופה, וזאת לאור השתכללות האיומים כמו גם הפתרונות. להלן מספר נקודות למחשבה ולהתייחסות עת גיבוש ההסדר בנושא, בתחומים שהם בעלי ידע ומיומנויות במכון.

התממה

הלשכה המרכזית לסטטיסטיקה מחזיקה בידיה מידע רב ואיכותי במגוון רחב של נושאים. מידע זה, הנאסף מגופים ציבוריים ופרטיים ומהציבור הרחב, הוא בעל ערך מחקרי וכלכלי רב, ויש בו כדי לסייע בניתוח תהליכים ומגמות הנוגעים לפעילות השלטונית והעסקית וההתנהלות האישית בישראל. לצד התועלות והיתרונות בהנגשת המידע אשר בידי הלשכה, טמון חשש משמעותי כי פרסום מידע רחב, גם אם יושמטו ממנו פרטים מזהים, יהיה מידע הניתן לזיהוי. לדוגמא, מחקר מקיף שנערך בארה"ב גילה שנתוני סקר האוכלוסין שנערך ב-2010 (המיקרו-דאטה) אשר פורסמו לציבור לאחר התממה בדרך של השמטת שדות מזהים, ניתנים לזיהוי ברמה של עשרות אחוזים ממשותפי הסקר.¹ הקושי בהפיכת קבצים בעלי מידע אישי לקבצים מותממים (שלא ניתן לחזור ולשייך את המידע שבהם לגורם אישי זה או אחר) מקבלים משנה תוקף עת הלשכה מבקשת להנגיש מידע גולמי ומפורט לצורך מחקר גם לחוקרים מחוץ ללשכה – פרקטיקה מקובלת במדינות רבות. על מנת להתמודד עם קושי זה, נדרש לעשות

¹ Groshen, E. L., & Goroff, D. (2022). Disclosure Avoidance and the 2020 Census: What Do Researchers Need to Know? *Harvard Data Science Review*, (Special Issue 2), P. 11-12. <https://doi.org/10.1162/99608f92.aed7f34f> (להלן - Groshen & Goroff)

שימוש בכלים שיש בהם כדי לצמצם עד מאוד את הפגיעה הפוטנציאלית בפרטיות תוך שימוש בטכנולוגיות מקדמות פרטיות (PET), ועל ידי יצירת תהליכים מבוקרים של הנגשת המידע והפיקוח.

בעבר די היה בהשמטת הפרטים המזהים כדי ליצור התממה מספקת של בסיסי נתונים, אך כיום לאור היכולות הטכנולוגיות המתפתחות והמידע הרב הזמין ברשת (בין אם באופן חוקי ובין אם באופן שאינו חוקי), נדרש יישום של שיטות התממה חדשות ומורכבות יותר שיספקו רמה הולמת של הגנת פרטיות לאנשים אשר מידע עליהם נאסף מכח החוק על ידי רשות ממשלתית.

למרות ששיטות התממה פוגמות בדיוק של הנתונים מכיוון שהן מכניסות שינויים בקובץ הנתונים, לאור הסיכונים בהנגשת המידע ללא התממה מקדימה, באופן שהיה מאיין את היכולת של הלשכה לתת גישה לנתונים בכלל, אין מנוס משילוב פרקטיקות של התממה טרם מתן גישה לנתונים.

יש לזכור עוד, כי גם בעבר בעת הכנה של נתונים סטטיסטיים ופרסומם, נכלל מרכיב של הערכה ותיקונים סטטיסטיים אשר נדרשו עקב אופיים של סקרים ומחקרים סטטיסטיים, ובוצעו פעולות התממה במידע, כך שאין בביצוע התממה הכנסה של פרקטיקה חדשה לגמרי אלא פיתוח וקידום של אמצעים במסגרת עקרון מקובל².

ויש להדגיש, התממה לעולם לא תוכל להבטיח הגנה מלאה על אי זיהוי כלל הגורמים הפרטיים עליהם יש מידע בקובץ. יחד עם זאת, טכנולוגיות הגברת פרטיות (PET) פועלות לייצר הגנה מספקת ביחס להערכת הסיכונים בקובץ קונקרטי. מכאן כי לא ניתן לדבר על פתרון יחיד והכרעות דיכוטומיות בלבד.

הערכה חישובית של רמת ההגנה שהתממה מספקת, אשר תאפשר ניתוח סיכונים וקבלת החלטות, יכולה להתבצע על בסיס רעיון ה'פרטיות הדיפרנציאלית', כפי שיפורט בהמשך.

זאת ועוד, יישום שיטות התממה טכנולוגיות הוא רק אחד ממעגלי ההגנה שניתן לספק לקבצי נתונים שיש בהם ערך לתועלת הציבור וקידום המחקר. ישנם כלים נוספים שיפורטו בהמשך אשר יכולים להציע בקרות מפצות ולהעלות את סך ההגנה, כלומר להוריד את רף הסיכון, לזיהוי של אנשים פרטיים מתוך קבצי נתונים שהונגשו³.

² Groshen & Goroff, p. 4 & 6

³ [Using Health Data for Research: Evolving National Policies](#), L. Shmerling-Magazanik (ITPI, 2021)

קובץ הנתונים

1. **גודל הקובץ** – מהו היקף הקובץ הן ביחס למספר נושאי המידע והן ביחס להיקף המידע הקיים על כל נושא מידע;
2. **איכות המידע** – עד כמה המידע איכותי ומדויק. לדוגמא, מידע אמפירי על הרגלי צריכה בפועל, לעומת מידע הנותן הערכה לגבי התנהלות צרכנית;
3. **מועד איסוף הנתונים ביחס למועד הפרסום** – ככל שהנתונים אשר מתבקש עליהם מידע ישן יותר, החשש לפרטיות יורד. את בחינת הזמן שחלף יש לאמוד מהנתון העדכני האחרון בקובץ הנתונים המבוקש.

אופן ההנגשה בהיבט הטכנולוגי

4. **אופן ההרשאה לקובץ הנתונים** – ישנן מספר מדרגות מרכזיות להנגשת מידע, מהמאובטח ביותר לפחות –
 - 4.1 נגישות בחדר מחקר פיזי;
 - 4.2 נגישות בחדר מחקר וירטואלי;
 - 4.3 העברת קבצים לקבוצה מסוימת;
 - 4.4 פרסום קבצים לציבור.
5. **אמצעי האבטחה** – מה הם אמצעי אבטחת המידע המשולבים במערכת ומצמצמים את האפשרות לניסיון לזיהוי חוזר של המידע. בעניין זה יש להבחין בין שני סוגים של אמצעי אבטחה –
 - 5.1 **אמצעים המצמצמים את היכולת באופן טכנולוגי** – כגון הקשחת הכוננים מהם יש נגישות למידע;
 - 5.2 **אמצעים שנועדו לניטור ובקרה בזמן אמת או בדיעבד** – כגון ניטור לוגים והתראה (או תיעוד) על שימוש חריג בנתונים. בעניין זה לא די בתיעוד כשלעצמו, יש צורך כי לאחראיים לבצע בקרה על אופן השימוש בנתונים, תהיה ההרשאה והנגישות לנתונים אלו על פי הצורך.
6. **חוסר יכולת להעתיק את הנתונים** – במקום בו רמת ההתממה אינה מספקת, אולם ישנם שיקולים אחרים המכריעים את הכף לטובת הנגשת הנתונים – כגון חשיבות המחקר ורמת המהימנות כמו גם אמצעי הפיקוח של הגורם המחקרי, יש לוודא באמצעים טכנולוגיים כי לא ניתן יהיה להעתיק את בסיס הנתונים, ולא להסתפק באמצעי פיקוח בלבד, המאפשרים תחקור ואכיפה בדיעבד, אך אינם מונעים את עצם האפשרות לזליגת מידע. כך למשל, כאשר הגישה לקבצים ניתנת בחדר מחקר פיזי אשר לא קיימת בו גישה לדואר אלקטרוני, אינטרנט או מדפסת.

בעל ההרשאה

7. **מספר המורשים** – ככל שמספר המורשים גדל, רמת הסיכון עולה. בעניין זה יש לתת את הדעת כי במקום בו ישנה חשיבות לשמירת מספר בעלי הרשאות מצומצם בלבד, אמצעי הכניסה למאגר יהיו כאלו המבטיחים כי האדם המורשה הוא מי שנכנס בפועל.
8. **מיקום הגורם המורשה** – ככל שהגורם המורשה יושב בישראל, יכולת הפיקוח עליו והכפפתו לדין ולנורמות הישראליות – גדל. ישנן מדינות (כגון: אוסטרליה וגרמניה) אשר מצמצמות את הנגישות למידע הסטטיסטי רק לחוקרים ולגופי מחקר היושבים בתחום המדינה, או מקשות בדרישות מחוקרים מחוץ למדינה.⁴ מבלי לנקוט עמדה בדבר נכונות התפיסה כי מידע שעובד בלשכה יהיה נגיש רק לחוקרים או גופי מחקר ישראליים, נוכח החשיבות לעתים של שיתופי פעולה בינלאומיים במחקר, גישה מסוג זה מקילה על אפשרות הפיקוח והאכיפה של קיום ההוראות.
9. **מורשה "ממוסד"** – ככל שהמורשה שייך לגורם מחקרי בעל מוניטין וניסיון בתחום המחקר, המחויב לפרקטיקות ולמשמעת התומכת בהגנה על בסיסי נתונים רגישים, הסיכון לשימוש לא מורשה, יורד.

הנתונים המשפיעים על סוג ההתממה הנדרשת, מגוונים ואינם חד משמעיים. מכאן כי לא ניתן לדבר על פתרון אחד, אלא על מקבץ פתרונות שצריכים להיות מותאמים לפי הערכת הסיכונים הקונקרטיים ובשים לב למקבצי נתונים נוספים שפורסמו או שיש כוונה לפרסם, אופן הנגשת המידע ולקהל היעד שיקבל גישה לנתונים. בעניין זה אנו ממליצים גם ללמוד מטיטוט חוזר מנכ"ל משרד הבריאות בנושא: "[הנחיות להתממת מידע בריאות לצרכי שימוש מחקרי](#)" (אוקטובר 2019).

פרטיות דיפרנציאלית

בשנים האחרונות מספר לשכות לסטטיסטיקה בעולם, מפרסמות את נתוני המיקרו-דאטה שלהן בהתבסס על התממת הנתונים באמצעי הגנת פרטיות שונים העונים על הרעיון של 'פרטיות דיפרנציאלית', מתודולוגיה חישובית המשמשת למדידת מידת המניעה של זיהוי חוזר של אנשים מתוך בסיסי נתונים.

בעניין זה ברצוננו להפנות את תשומת לבכם [לעבודה המקיפה](#) שנעשתה בנושא פרסום נתוני סקר התושבים בארה"ב לשנת 2020. בתהליך מעמיק ומקיף, החליטה הלשכה על פרסום הנתונים לציבור לאחר

⁴ בעוד שבאוסטרליה הרשאה של גופי מחקר מחוץ למדינה לנתוני מיקרו-דאטה תיבחן על בסיס בקשה פרטנית, בגרמניה גישה לקבצים מדעיים (Scientific Use Files) ניתנת לגופי מחקר גרמניים בלבד (נוסף על דרישת הימצאותם בגרמניה בעת הגישה לקבצים) וחוקרים ממכוני מחקר מחוץ לגרמניה יכולים לגשת לנתונים במרכזים המאובטחים או לקבל גישה לקבצים מוגבלים יותר. ראו [Federal Statistical Office of Germany - access to microdata](#).

שעברו התממה באמצעות אלגוריתם בתהליך סדור ומתועד המממש את תפיסת הפרטיות הדיפרנציאלית. יש לציין כי גם [באנגליה](#) ובאוסטרליה בחרו לפרסם את תוצרי הסקרים האחרונים בהתבסס על התממה מסוג (Cell key perturbation) שעונה על עקרונות פרטיות דיפרנציאלית.

לאור הנתיה בו הולכות מדינות אחרות, אנו ממליצות כי בעניין פרסום המיקרו דאטה לכלל האוכלוסייה, תפעל הלשכה על מנת להטמיע מתודות של פרטיות דיפרנציאלית בישראל.

יובהר עוד, כי בתפיסה זו מעוגן היחס בין רמת המניעה של זיהוי מחדש של אנשים על ידי החדרת "רעש" לנתונים לבין רמת השימושיות והדיוק של המידע לצרכי מחקר, בפרמטר המכונה 'אפסילון'. פרמטר זה מייצג מספר הניתן לבחירה בעת יישום האלגוריתם שנבחר ל"הרעשת" הנתונים, ולמעשה זהו פרמטר המאפשר "כיוול" של היחס בין הגנת פרטיות לדיוק נתונים, ומהווה בכל מקרה ומקרה הכרעת מדיניות.

את ועוד, רעיון הפרטיות הדיפרנציאלית מאפשר חישוב של סיכון הזיהוי מחדש גם עבור מערכת של קבצי נתונים המפורסמים או מונגשים, כך שיובא בחשבון הסיכון המצרפי של זיהוי מחדש בהתבסס על שילוב של אנליזות מצטברות על טבלאות שונות של נתונים. באופן זה מקובל לכוון את סך הסיכון לכלל הטבלאות המבוססות על נתוני מפקד האוכלוסין למשל, 'תקציב פרטיות'. ניהול תקציב זה, בהתבסס על בחירת אפסילון מסוים, יאפשר מטריית הגנת פרטיות מתמשכת לנתונים שהונגשו לציבור.

יצוין, כי במסגרת הפרוייקט של הלמ"ס בארה"ב למפקד אוכלוסין 2020, נתבצעה בחינה של הטבלאות שפורסמו בעבר, ונשאלה השאלה האם כולן אכן רלוונטיות לציבור החוקרים, ומי מהן נמצאות בשימוש רב לעומת שימוש נמוך. זאת מאחר שככל שמפורסם יותר מידע, יותר טבלאות נתונים, תקציב הפרטיות המבוסס על האפסילון הנבחר מצטמק. ככל שישנם נתונים שאינם נדרשים עוד או בשימוש נמוך במיוחד, ייתכן שעדיף שלא לפרסמם על מנת שלא לבזבז שלא לצורך את תקציב הפרטיות.⁵

דרישות ממקבלי הנגישות למידע

על מי שביקש לגשת לנתונים, מוטלת אחריות רבה. האפשרות של הלשכה להתיר נגישות למידע שיש בו מן הפגיעה בפרטיות על בסיס האיזון בין זכות זו לחשיבות המחקר בישראל, צריכה להתבסס גם על מהימנות הגוף המורשה לקבל מידע, ועל היכולות לפקח ולאכוף עליו את ההסדרים שנקבעו.

לפיכך יש מקום להציג דרישות מקדימות למבקשים לקבל נגישות למידע פרטי המוחזק בידי הלשכה. בין היתר מוצע לבחון את הנושאים הבאים –

⁵ Groshen & Goroff, p. 19-21

1. לחוקר המבקש יש ניסיון רלוונטי ומוכח בביצוע מחקרים מבוססי נתונים. במדינות שונות יש דרישות סף כגון תואר אקדמי מתקדם, ידע במחקר אמפירי ובסטטיסטיקה, הצגת עבודות מחקר קודמות וכד'.⁶
 2. מעבר לשאלת היכולות של החוקר עצמו, רצוי להתנות השתייכות למוסד מחקרי מוכר. השתייכות זו יש לה שני יתרונות – קיומו של מנגנון סדור לשמירה על המידע ועל אתיקה מחקרית, ויכולת לייצר אכיפה אפקטיבית במקום בו יתבצע שימוש לא מורשה – הן בשל החשש של המוסד שאירוע מסוג זה עשוי לפגוע בקבלת הרשאות שיתבקשו בעתיד, והן לאור מנגנוני הדין המשמעתיים הקיימים בתוך גוף מחקרי אל מול עובדי המוסד. על המוסד להוכיח כי הוא מחזיק במדיניות רלוונטית ביחס להתממת בסיסי נתונים מחקריים, נהלי אבטחת מידע, ומערכת פיקוח ואכיפה על החוקרים.
 3. ישנה חשיבות גם להיסטוריה המוכרת של המוסד והחוקר. מקום בו היה בעבר שימוש ללא הגנה מספקת על המידע האישי, והאופן בו המוסד התמודד עם אירועים מסוג זה – צריכים להוות שיקול לחיוב ולשלילה בשאלת מידת המידע הרגיש שיאושר לחוקר ולמוסד להיות נגישים אליו.
 4. יש להגביל את ההרשאות שניתנו למידע בתקופת זמן, המינימלית הנדרשת, ובכל מקרה לקבוע כי אחת ל-3-5 שנים תבחן הלשכה מחדש את ההרשאה.⁷ בבחינה מיוחדת של ההרשאה נדרש לבחון כי לא היו שינויים בנסיבות אשר אפשרו את מתן ההרשאה, אך גם לתת את הדעת לשימוש בפועל במידע ולהתקדמות המחקר. ככל שלא נעשה שימוש בפועל, ללא הצדקה, או במקום בו נדמה כי אין התקדמות מחקרית, תהא זו עילה טובה לשקול אם לחדש את ההרשאה של החוקר או המוסד האקדמי.
 5. ישנן מדינות המתנות את הנגישות למידע רגיש, במיקום של החוקר וגוף המחקר באותה מדינה, כמזכר לעיל ביחס לבעל ההרשאה (סעיף 8). גם אם הכרעה זו מעוררת שאלות ביחס לחשיבות החופש האקדמי ותרומתם של חוקרים מחוץ לישראל גם למחקר בישראל, נדמה כי לכל הפחות בהקשר לאפשרות לאכיפה יעילה יש לשקול הוראה דומה גם בדין הישראלי החדש.
- ויובהר, ההרשאה צריכה להנתן הן למוסד והן לחוקר, אולם הם אינם תלויים בהכרח זה בזה, והמוסד האקדמי, באישור הלשכה, רשאי לדוגמא לשנות את החוקר המוביל במחקר לגביו נתבקשה ההרשאה.

⁶ בריטניה ואוסטרליה, למשל, קובעות תנאי סף של שלוש או חמש שנות ניסיון (בהתאמה) במחקר כמותי, או תואר ראשון ומעלה עם רכיב משמעותי של לימודי מתמטיקה או סטטיסטיקה.

⁷ כך נהוג גם במדינות שונות. לדוגמה, בבריטניה, הרשאה ניתנת בנפרד לחוקר מורשה ולמחקר מורשה. הרשאה ניתנת לתקופה של עד חמש שנים במסגרתה יתבצעו הערכות תקופתיות הן ביחס לחוקר ולמחקר, והן ביחס לאיומים ואתגרים חיצוניים המצדיקים את שינוי התנאים לקבלת הסמכה. כאמור, גם כאשר חוקר הינו בעל הסמכה, עליו להגיש כל מחקר לאישור בנפרד. ראו: UK Research Code of Practice and Accreditation Criteria. גם בארה"ב ניתנת גישה לנתונים לחוקר רק לאחר הגשת בקשה הנבחנת ע"י הלמ"ס ועמידה בקריטריונים.

בעלי הרשאות נוספים

בעניין הנגישות למידע יש לתת את הדעת גם למי שנגישים למידע שלא למטרות מחקר, לדוגמה קבלני משנה הפועלים לתחזק או לתפעל את מערכות המידע, או גורמים שיינתן להם גישה לצורך יצירת ההתממה. בניגוד לעובדי הלשכה עצמה, על עובדי חברות במיקור חוץ לא חלים הוראות סודיות ייעודיות והם אינם כפופים לדיון המשמעותי כעובדי המדינה. לפיכך יש צורך לוודא שהחקיקה נותנת את המסגרת הנורמטיבית הקובעת את המסגרת שמטרתה לצמצם את הנגישות של גורמים אלו למידע האישי, יצירת אמצעי סינון קפדניים מראש, כמו גם יצירת מסגרת פיקוח ואכיפה אפקטיביים.

הנגשת המידע המינימלי הנדרש

עקרון נוסף שחשוב שיעוגן בחקיקה, הוא העקרון כי לבעלי הרשאה למידע, יוגש המידע המינימלי הנדרש. האחריות לבסס את הצורך במידע האישי לצורך המחקר, היא של החוקר והגוף המחקרי. ככלל, מידע עשיר יותר עשוי להפיק תובנות רבות יותר – כולל תובנות שלא ניתן היה לצפות מראש. עם זאת, בשל העובדה כי התממה היא שאלה של הערכת סיכונים ואינה מספקת הגנה מוחלטת, ראוי כי החוקר יידרש לנמק את הצורך שלו במידע המקיף, וכי האישור שיינתן לו יהיה למידע המינימלי הנדרש לצורך המחקר – ולא למידע המקסימלי.

אמצעי פיקוח

מזעור הנזק

יש להעדיף פתרונות בהם במקום בו מתגלה שימוש לא מורשה, ניתן יהיה להפסיק את הנגישות באופן מיידי. גם במובן זה יש יתרון לחיבור החוקרים לחדר מחקר וירטואלי או פיזי על פני העברת קבצים מחוץ ללשכה, באופן שמקטין את יכולת מניעת או צמצום הנזק.

סנקציות

יש לקבוע אפשרות להטיל סנקציות על מי שהפר את תנאי השימוש. יש לבחור כלי אכיפה שאינם מתמקדים רק בהליך הפלילי – הארוך והמורכב להוכחה. יש להוסיף אפשרות להטלת עיצומים כספיים כמו גם להתנות

אישורים חדשים להנגשת מידע באי קיומן של הפרות קודמות. לשם השוואה, בארצות הברית כפופים בעלי גישה למידע שאינם עובדי הלשכה לסנקציות של קנס משמעותי ואף תקופת מאסר.⁸

לצורך כך ישנה חשיבות לנהל רישום של הגורמים המפרים. רצוי שפרסום זה יהיה נגיש לציבור על מנת שגורמים עתירי ידע אחרים שעלולים להתקשר עם מוסדות מחקר או חוקרים, יידעו להשמר במקרה הצורך.

בקה מקדימה לפרסום מחקר

במספר מדינות נהוג כי טרם פרסום המחקר, מועבר המחקר לעיון הלשכה על מנת לבחון כי אין הנתונים המוצגים במחקר מאפשרים זיהוי של הפרט.⁹ הסדר כאמור מייצר חשש להתערבות בחופש האקדמי, כמו גם עלול לייצר בירוקרטיה מיותרת ומכבידה.

בכל תהליך שייבחר בסופו של יום על ידי הלשכה, מומלץ ליצור מנגנון היוועצות עם הלשכה מקום שבו החוקר או מוסד המחקר מתלבטים בסוגיות ושאלות של התממה. ככל שהלשכה תבחר לשמר מקרים חריגים בהם תנתן נגישות למידע רגיש רב שלא דרך חדרי המחקר הווירטואלים (פרקטיקה שאנו ממליצים שתשקל רק במקרים בהם הערך המחקרי לתועלת הציבור הוכח כגבוה והחיוניות בביצוע המחקר מחוץ לחקר המחקר המוגן הוכחה), יש לשקול יצירת פרקטיקה כאמור. יש לוודא ולהקפיד כי המנדט של הלשכה בעניין זה יהיה אך ורק לבחינת שאלת התממת הנתונים, ולא תגלוש לשאלות או מתודות מחקריות אחרות.

שקיפות

יש חשיבות כי הלשכה תפעל בשקיפות מרבית. שקיפות זו נדרשת בנושאים הבאים –

1. הסטנדרטים שייקבעו על ידי הלשכה למתן נגישות למידע אישי;
2. הכללים והמתודות להתממת מידע;
3. הגורמים שקיבלו הרשאת שימוש במידע;
4. אירועים של שימוש לא מורשה במידע לרבות שם הגורם המפר והפעולות שננקטו כנגדו.

⁸ראו Title 13, U.S. Code

⁹ בגרמניה, למשל, נדרש להגיש את המחקר אשר מבוסס על נתונים במרכזי הלשכה לאישור טרם פרסומו על מנת לוודא כי הוא אינו מאפשר גילוי פרטים אישיים. ראו: Regulations on the analysis of microdata כך גם בארה"ב, שם הוצאת כל תוצר מחקר - טבלה, תרשים וכו' - נבחנת ע"י הלמ"ס בטרם מתן אישור להוציאה. בהקשר של נתוני מפקד אוכלוסין 2020 אף הוסיפו את תוצאות הבחינה הזו לתקציב הפרטיות של הפרויקט כולו ומפחיתים לפי הצורך את התקציב ככל שניתן אישור להוצאת תוצרי מחקר שהוספתם לגוף המידע הגלוי יש כדי להגדיל את הסיכון לזיהוי חוזר של אדם מהמידע. Groshen & Gorof, p. 34.

חשיבות השקיפות של הלשכה מול הציבור גבוהה במיוחד היות שרגישות הציבור לנושא פרטיות המידע האישי התחדדה מאד בעת האחרונה, והיכולת של הלשכה להמשיך ולאסוף מידע מפורט ורב מהציבור תלויה בשיתוף הפעולה של הציבור עם פועלו. חשיפה של מידע אישי עשויה לפגוע קשות באמון הציבור ובנכונותו לשתף פעולה ולמסור מידע למדינה.

עקרונות מנחים בחקיקה להנגשת מידע – סיכום

לאור האמור לעיל להלן סיכום של העקרונות שאנו ממליצות לעגן בחקיקה ראשית או בהסדר משני. יובהר כי העקרונות המוצעים אינם מכסים את כלל הנושאים שהוצגו במסמך של הלשכה או שנדרשים בחקיקה מחדשת בתחום הסטטיסטיקה, אלא את אלו שיש למכון מומחיות לגביהם. לאור אופן ניסוח הפנייה על ידי הלשכה, העקרונות מנוסחים בקווים כלליים בלבד.

עקרונות שיש לעגן בחקיקה ראשית

1. המחויבות של הלשכה להגן על המידע הפרטי ולפעול למניעת זיהוי מידע אישי אודות אדם.
2. חשיבות הנגשת מידע לציבור ולחוקרים – בשים לב למגבלות ולהגנות על מידע פרטי, בטחוני ומסחרי.
3. לא יונגש מידע לציבור או לחוקרים שאינם עובדי הלשכה, אלא אם בוצעה התממה בבסיס הנתונים כפי שייקבע בוועדה ייעודית לנושא, הכוללת נציגי ציבור. הוועדה תהיה אמונה על בחינת ואישור המתודות להנגשת מידע מותמם ותגדיר את הכללים והעקרונות לניהול הסיכונים בהנגשת המידע על ידי הלשכה (להלן הוועדה).
4. בבחינת פתרונות להתממת מידע על הלשכה והוועדה לתת דעתם לסוגיות הבאות –
 - 4.1 גודל הקובץ ואיכות המידע;
 - 4.2 הקבצים הנוספים שיפורסמו מתוך אותו בסיס מידע גולמי שבידי הלשכה;
 - 4.3 אופן מתן ההרשאה המבוקש;
 - 4.4 האמצעים הטכנולוגיים בהם נעשה שימוש לצמצום האפשרות לשימוש לא מורשה במידע;
 - 4.5 אמצעי האבטחה אצל הגורם מקבל המידע;
 - 4.6 מיהות הגורם המורשה ומספר האנשים להם תנתן הרשאה;
5. עקרונות ההתממה יגובשו בכללים שיונגשו עד כמה שניתן לציבור.
6. עקרונות ההתממה ייבחנו לכל המאוחר אחת לשלוש שנים.
7. הגורם המוסמך לתת הרשאה למידע ייתן דעתו, בין היתר, לנתונים הבאים טרם מתן הרשאה –
 - 7.1 מיהו החוקר והמוסד המחקרי המבקש את ההרשאה;

- 7.2 לשם מה נועד המחקר;
- 7.3 מהו אופן הנגישות למידע;
- 7.4 מהו סוג ההתממה שהקובץ עבר.
8. המידע שיונגש לחוקר יהיה המידע המינימלי ביותר הנדרש לצורך המחקר;
9. מתן הרשאת נגישות למידע תנתן לתקופה של עד 3 שנים, וניתנת להארכה. בעת ביצוע ההארכה יבחן הגורם המורשה מטעם הלשכה –
- 9.1 אי שינוי בנסיבות על בסיסם התקבל ההיתר;
- 9.2 האם נעשה שימוש בפועל בנגישות שניתנה לצרכי קידום המחקר.
10. מתן מענה למחויבות גורמים הפועלים במיקור חוץ לצרכים תפעוליים, ובכלל זה הוספת אכיפה אפקטיבית, הטלת עיצומים ומתן ערובה, להבטחת הציות להוראות.
11. הלשכה תקבע בכללים מה הם אמצעי הפיקוח שיוטלו על מי שקיבל נגישות למידע אשר בלשכה.
12. ייקבעו הוראות המחייבות את הלשכה בשקיפות ביחס לנושאים הבאים –
- 12.1 הכללים למתן נגישות למידע אישי;
- 12.2 הכללים והמתודות להתממת מידע;
- 12.3 הגורמים שקיבלו הרשאת שימוש במידע;
- 12.4 אירועים של שימוש לא מורשה במידע לרבות שם הגורם המפר והפעולות שננקטו כנגדו.

עקרונות שיש לעגן בהסדר משני

1. הנגישות למידע רגיש המצוי בידי הלשכה על ידי חוקרים מורשים, יתבצע באמצעות חיבור לחדרים וירטואליים.
2. נתונים שיונגשו לציבור יעברו התממה העונה על תפיסת הפרטיות הדיפרנציאלית, ופרמטר אפסילון ייקבע על ידי הוועדה המקצועית שתוסדר בחקיקה ראשית.
3. הלשכה תמשיך ותתעדכן בהתפתחויות בשיטות הגנה על פרטיות המידע ותבחן כלים טובים יותר או מתאימים יותר.
4. בכללים שייקבעו יש לקבוע תנאים הבוחנים את האמור בפרק הנוגע ל"דרישות ממקבלי הנגישות למידע".
5. אמצעי הפיקוח ייקבעו בהסדר משני לאור היכולות המשתנות בתחום זה.

אנו מודות לכם על פנייתכם, ומקוות כי האמור במסמך זה יהיה לכם לעזר.

נשמח להרחיב ולסייע ככל שנדרש.

בברכה,



לימור שמרלינג מגזניק

מנהלת המכון



עו"ד רבקי דב"ש

עמיתה בכירה במכון