מאמר זה פורסם בכתב העת "חידושים בניהול", גיליון מס' 7, אוקטובר 2020,
היוצא לאור על ידי הפקולטה לניהול על שם קולר באוניברסיטת תל אביב.

הפקולטה לניהול
ע"ש קולר
אוניברסיטת תל אביב

סוגיות אתיות בטכנולוגיות ביג דאטה

אהרונה ספר

ד"ר אהרונה ספר היא מרצה בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. סיימה תואר ראשון בניהול ובמדע המדינה באוניברסיטת תל אביב והשלימה תואר שני ודוקטורט בחקר ביצועים בפקולטה לניהול ע"ש קולר. היא מלמדת את הקורס "היבטים אתיים בתחום הביג דאטה" לתלמידי התואר השני במינהל עסקים, וכן את קורסי היסוד בחקר ביצועים בתוכנית התואר הראשון בפקולטה.

תקציר

טכנולוגיות ביג דאטה המשולבות בתהליכי איסוף וניתוח של נתונים, נמצאות כיום בשימוש במגוון רחב של תעשיות ויישומים. יתרונותיהן ברורים – ארגונים יכולים להכיר טוב יותר את הלקוחות שלהם, התנהגותם וצורכיהם, לקבל החלטות מבוססות נתונים, לייעל תהליכים על ידי ביצוע פעולות בצורה אוטומטית, ועוד. לצד היתרונות נשמעים גם קולות המבקרים את השימוש בטכנולוגיות אלו בשל בעיות אתיות שונות, המשתקפות במקרים הולכים ומתרבים של פגיעה בפרטיות, טעויות והטיות. מאמר זה מציף את הסוגיות האתיות הללו וסוקר כלים שונים, טכנולוגיים וארגוניים, שבהם ארגונים יכולים להשתמש כדי להתמודד עם הבעיות ולאזן בין היתרונות לבין הסיכונים שבטכנולוגיות.

מבוא

הצורך במסגרת אתית בעת יישום טכנולוגיות ביג דאטה נובע מקיומן של דילמות מוסריות שמעמתות את היתרונות של הטכנולוגיה עם הסכנות הטמונות בה. למשל, שמירה על בריאות הציבור או על הביטחון הלאומי אל מול הזכות לפרטיות, או קִדמה טכנולוגית אל מול שוויון והיעדר אפליה. לדוגמה, מגפת הקורונה ממחישה את הצורך שלנו בטכנולוגיות המסתמכות על ביג דאטה – איסוף נתונים לצורך מעקב ואיתור מגעים וניתוחם לצורך ניהול אפידמיולוגי חכם ויעיל. מנגד, המגפה חשפה גם את הבעייתיות האתית הכרוכה בשימוש בטכנולוגיות הללו: המתח בין הצורך במעקבים לבין השמירה על הפרטיות, וכן היעדר מסגרת אתית להפעלתם של כלי בינה מלאכותית שמקבלים החלטות באופן אוטונומי.

מאמר זה סוקר את הבעיות העולות בעת יישומן של טכנולוגיות ביג דאטה, החל משלב איסוף הנתונים והחזקת מאגר הנתונים, ועד לשימוש בדאטה לצורך קבלת החלטות. יש לציין כי המאמר מתייחס לסוגיות האתיות שעולות משימוש בטכנולוגיות ביג דאטה המסתמכות על נתונים של משתמשים אנושיים (Human Subjects). אין כאן עיסוק בהיבטים של האתיקה של המכונה (כגון החלטות ממוכנות של מכוניות אוטונומיות ורובוטים).

לפני כ-35 שנה פורסם מאמרו של מייסון: Four Ethical Issues of the Information Age (Mason, 1986) שהתייחס לסוגיות האתיות המשמעותיות בעידן המידע. המאמר דן בארבע סוגיות, שקיבלו את ראשי התיבות PAPA:

- פרטיות (Privacy): בעידן שבו מתקיים איסוף נרחב של מידע אישי, יש לקבוע כללים שיסדירו איזה מידע אישי חייב אדם לחשוף בפני אחרים, באילו תנאים ותחת אילו מגבלות; ואיזה מידע יכול אדם לשמור לעצמו בלי שייכפה עליו לגלותו.
- דיוק (Accuracy): ההסתמכות הרבה על מערכות מידע מחייבת לקבוע מי אחראי לדיוק ולנכונות של המידע, ומי אחראי לטעויות, לחוסר דיוק, ובעיקר לנזקים שנגרמים בשל כך.
- בעלות על הנתונים (Property): ערכם הגבוה של הנתונים בעידן זה מעלה את השאלות למי שייך המידע, האם ניתן לסחור בו ומה המחיר ההוגן שלו.
- גישה (Access): איסוף וטיפול במידע אישי, שהוא לעיתים רגיש, מחייבים לקבוע איזה מידע אדם או ארגון רשאים להחזיק ומהם התנאים והמגבלות על כך.

בחלוף 35 שנים מפתיע לראות עד כמה סוגיות ה-PAPA רלוונטיות גם היום, בעידן הביג דאטה. ההקשר אומנם השתנה, אבל העקרונות נותרו דומים.

מאמר זה עוסק בעיקר בשתי הסוגיות הראשונות, הפרטיות והדיוק, כפי שהן באות לביטוי בשני הרבדים העיקריים בשימוש בביג דאטה – מאגר הנתונים וניתוח הנתונים, כמתואר באיור מס' 1.

איור 1: רובדי השימוש בביג דאטה והסוגיות האתיות המתעוררות בהם

רובד I – מאגר הנתונים

- איסוף הנתונים
- החזקת הנתונים ואבטחתם
- הפצה ושיתוף של נתונים

סוגיות:

הזכות לפרטיות
אמון

רובד II – ניתוח הנתונים

- ניתוח והפקת תובנות
- קבלת החלטות מבוססת AI

סוגיות:

דיוק הנתונים
ותוצאות הניתוחים

הרובד הראשון, **רובד מאגר הנתונים**, כולל את תהליכי איסוף הנתונים אודות לקוחות ומשתמשים, ההחזקה והאבטחה של הנתונים, וכן הפצה ושיתוף של הנתונים. ברובד זה אנחנו מזהים בעיקר סוגיות של פגיעה בפרטיות ובאמון. למשל, משתמשים שאינם מודעים להיקף הנתונים האישיים שנאסף לגביהם, או שהצלבת מאגרי נתונים חושפת מידע אישי שלא התכוונו לשתף. כמו כן, היחסים הא-סימטריים בין בעל מאגר הנתונים (שבידיו השליטה על האינפורמציה הפרטית של אנשים רבים) לבין הלקוחות והמשתמשים, גורמים לכך שהאחרונים מאבדים דה-פקטו את הבעלות על הנתונים שלהם עצמם.

הרובד השני, **רובד ניתוח הנתונים**, כולל את תהליכי ניתוח הנתונים והפקת תובנות אודות המשתמשים, וכן שימוש באלגוריתמים ובמערכות בינה מלאכותית (AI) המפיקים ידע נוסף מן הנתונים ומאפשרים קבלת החלטות אוטומטיות. ברובד זה מתעוררות שאלות לגבי מידת הדיוק של הנתונים או של תוצאות הניתוח שלהם. כמו כן, נעשה שימוש באלגוריתמים שמסוגלים לקבל החלטות אך הם פועלים כ"קופסה שחורה". כלומר לא תמיד ברור על סמך איזה מידע התקבלו ההחלטות וכיצד פועל האלגוריתם, ויש מחלוקת אם ניתן לשחזר את דרך קבלת ההחלטות ולספק עבורן הסבר. נוסף על כך, ברובד זה ניתקל בבעיות מהותיות של חוסר דיוק, כגון טעויות, הטיות ואף אפליה של אוכלוסיות, שמקורן בשלבים שונים של תהליך למידת הנתונים וקבלת ההחלטות.

בפרקים הבאים נרחיב על שני הרבדים ועל הבעיות השונות המתעוררות בהם, ונעסוק בהתייחסות הנדרשת מהארגון ובכלים העומדים לרשותו.

רובד I – מאגר הנתונים

בעידן הביג דאטה קיבלו הנתונים את הכינוי "הנפט החדש", משום שהדעה הרווחת היא שככל שיהיו לנו יותר נתונים, כך נוכל להפיק יותר תובנות ולייצר יותר ערך לארגון. לפיכך התפיסה היא שתמיד כדאי לאסוף ולשמור כמה שיותר נתונים, גם אם לא ברור היום מה יהיה השימוש בהם בעתיד.

בהתאם, איסוף הנתונים עומד בבסיס הרובד של מאגר הנתונים. ארגונים שונים נוקטים שיטות איסוף שונות ונוהגים בנתונים במידות שונות של שקיפות. רוב הארגונים שומרים את נתוני האינטראקציה עם הלקוחות, כמו פרטי רכישות, מועדי התקשרויות וכדומה (לדוגמה, שמירת נתוני מועדון לקוחות). לעיתים נשמרים גם נתונים מקיפים יותר, הכוללים נתונים ממקורות מגוונים או נתונים עקיפים. כך למשל, חברות יכולות לשמור מידע אודות מאפיינים אישיים של לקוחות שכלל לא נמסרו על ידם, אלא הוסקו מניתוח ההתנהגות שלהם ברשתות חברתיות, כגון הפוסטים שהגיבו עליהם והתמונות שפרסמו. בנוסף, חברות רבות מבצעות מעקב אחר הרגלי הגלישה של לקוחותיהם (Gebhart, 2018).

רובד מאגר הנתונים כולל גם את החזקת הנתונים בארגון ואבטחתם. בהקשר זה עולה השאלה אם נתונים שנאספים ממקורות שונים נשמרים באופן מבוזר או מאוחדים למאגר אחד. מאגרי המידע של עירייה, למשל, יכללו נתונים רבים על התושבים, הנאספים באגפים שונים (כגון תשלומי ארנונה וחינוך). במקרה כזה חשוב לשמור על המאגרים הללו נפרדים כדי למנוע, למשל, אפליה של תלמידים בשל חובות הוריהם לעירייה. בארגון עסקי, לעומת זאת, תהיה נטייה לבצע אינטגרציה של כמה שיותר נתונים אודות הלקוחות, כל עוד אין מניעה ברורה לעשות זאת.

החזקת הנתונים נוגעת גם למדיניות האבטחה שלהם בארגון. מדיניות זו כוללת אמצעי אבטחה למניעת חדירה אל מערכות הארגון, קווים מנחים בנוגע להרשאות הגישה אליהם (מי רשאי לגשת לאילו נתונים והאם הנתונים נחוצים לצורך ביצוע עבודתו), וכן יישום של שיטות שיבטיחו את שמירת הפרטיות במקרה של פריצה אל הנתונים מחוץ לארגון או גישה לא מורשית מבפנים. שיטה מקובלת אחת היא התממה (De-Identification או Anonymization), הכוללת הסרת פרטים מזהים ממאגר מידע כך שזהות האנשים במאגר נשארת אנונימית. קיים מנעד רחב של מידת **ההתממה** של נתונים, החל מהסרת פרטים מזהים ישירים בלבד, כגון שם, מספר תעודת זהות וטלפון, דרך מיסוך חלקי של נתונים, כגון הצגת שתי ספרות ראשונות בלבד מהמיקוד, הצגת שנת לידה בלבד ולא תאריך מלא, ועד הצפנת נתונים מסוימים כאשר רק לבעל המאגר יש את המפתח לשחזורם. מידת ההתממה תשפיע כמובן על ההסתברות לזיהוי מחדש (Re-Identification) של אדם שפרטיו נמצאים במאגר.

לעיתים הרובד של מאגר הנתונים יכלול גם את מדיניות הארגון בנוגע להפצה ושיתוף של נתונים עם גורמים שלישיים לצורכי ניתוח ושיתוף ידע. לדוגמה, קבלת הסכמה מלקוחות הארגון להעברת נתונים אודותיהם ולביצוע התממה או פעולות אחרות על הנתונים לפני הפצתם.

סוגיות אתיות ברובד מאגר הנתונים

הסוגיות האתיות המהותיות שנוגעות לתהליכים ברובד מאגר הנתונים הן פרטיות ואמון.

פרטיות. הסוגיה המרכזית והמדוברת ביותר היא החשש לפגיעה בפרטיות הלקוחות ומכאן גם באמון שלהם בארגון. הזכות לפרטיות מוגדרת כזכות של אדם להגדיר סביבו מרחב שכולל את כל הדברים השייכים לו: גופו, ביתו, רכושו, מחשבותיו, סודותיו וכדומה. במסגרת מרחב זה, הזכות לפרטיות היא היכולת של הפרט לבחור אילו חלקים במרחב יהיו נגישים לאחרים, באיזה אופן ותחת אילו מגבלות (Birnhack and Elkin-Koren, 2005).

הזכות לפרטיות מתערערת במקרים רבים. איסוף הנתונים מתרחש לעיתים ללא ידיעת המשתמשים (Lynskey, 2019) או בלי הסכמתם. כך למשל, במהלך משבר הקורונה, בשל הצורך לשמור על בריאות הציבור, נאספים נתוני מיקום של אזרחים, נחשפים פרטים של חולים ומבוצע מעקב אחר מבודדים. למעשה נתוני מיקום נאספים כל העת אצל הספקיות הסלולריות וכן במגוון אפליקציות המותקנות בטלפון הנייד, בין אם נתוני המיקום נדרשים לשם פעולתן ובין אם לאו (Valentino-DeVries et al., 2018; Nakashima, 2018). סדרה של מחקרים הראתה כי נתוני מיקום הם רגישים ואישיים ביותר, ובמקרים רבים ניתן לבצע שחזור וזיהוי מחדש גם של נתוני מיקום אנונימיים (de Montjoye et al., 2013; Douriez et al., 2016). הטענה היא כי לא ניתן כלל לתאר נתוני מיקום כאנונימיים, משום שכאשר הם מדויקים מאוד ומתעדים מיקום של הפרט לאורך זמן ממושך הם בלתי אפשריים להתממה. למעשה, יש הטוענים ש-DNA הוא הדבר היחיד שקשה יותר להתממה (Thompson and Warzel, 2019).

החשש לפרטיות הלקוחות מתעורר גם בעת שיתוף הנתונים או הפצתם. טכנולוגיות ביג דאטה וההבנה שבכוחן לספק פתרונות חדשים במגוון תחומים, מחזקות את הדרישה לשתף את המידע הרב שנאגר הן בגופים ממשלתיים והן בחברות פרטיות. דוגמה לכך ניתן לראות בפרויקט הלאומי הישראלי לפתיחה ושיתוף מאגרי המידע של קופות החולים עם חוקרים באקדמיה ועם חברות טכנולוגיה, במטרה לקדם את תחום הבריאות הדיגיטלית בישראל, לשפר את שירותי הבריאות, ובה בעת גם לחזק את התעשייה ואת האקו-סיסטם הישראלי (תוכנית לאומית לקידום תחום הבריאות הדיגיטלית כאמצעי לשיפור הבריאות וכמנוע צמיחה, 2018). לצורך כך הגדירה המדינה תקנות לשימוש מחקרי במידע הרפואי, המתייחסות בראש ובראשונה לשמירה על פרטיות החולים. התקנות כוללות, בין היתר, קבלת הסכמה מאדם כדי להעביר את נתוניו אם לא הותממו, התממת הנתונים, ניתוח הנתונים על ידי מורשים בלבד ובסביבה שהיא באחריות הגוף שאסף את הנתונים, ומתן אפשרות לבקשה להיגרע ממאגר הנתונים (תקנות שימוש מחקרי במידע בריאות, 2019).

גם חברות פרטיות משתפות פעמים רבות את הנתונים שלהן עם חברות חיצוניות ממניעים עסקיים שונים ולצורכי מחקר פנימיים. דוגמאות בולטות לכך הן אפליקציות שמוכרות מידע לפייסבוק ומידע רפואי שנמכר לחברות ביטוח. במקרים כאלה גובר החשש לפרטיות בשל היעדר שקיפות מספקת של התהליכים.

בישראל, בהתאם לחוק הגנת הפרטיות, ארגון המבקש להעביר את הנתונים לגורם חיצוני נדרש לקבל את הסכמת נשואי המידע (חוק הגנת הפרטיות, 1981; בירנהק, 2018). אולם דרישה זו אינה קיימת כאשר מאגר הנתונים איננו כולל מידע מזהה, או שלא ניתן לזהות באמצעותו את הפרט, כלומר מידע מותמם. החרגה זו עלולה ליצור בעיה כאשר המידע עוזב את הארגון ומגיע לסביבה אחרת הכוללת מאגרי נתונים נוספים רבים, משום שאז גם נתונים שעברו התממה יכולים לעבור זיהוי חוזר באמצעות הצלבה עם מקורות המידע האחרים. כך קרה, למשל, כשחברת נטפליקס פרסמה נתוני צפייה אנונימיים כביכול של משתמשים, וחוקרים הצליבו את מועדי הצפייה עם ביקורות שהתפרסמו באתר אחר. בשיטה זו הם הצליחו לשחזר את זהות המשתמשים ולחשוף בין היתר נטיות מיניות והעדפות שונות שלהם (Narayanan and Shmatikov, 2008).

כאמור, בתחום הרפואי נערכים בארץ להוצאה לפועל של התוכנית לשיתוף מאגרי המידע הרפואיים של קופות החולים. אולם חשוב לזכור שברחבי העולם קרו לא מעט מקרים שבהם פורסמו מאגרי מידע רפואיים לצורכי שיתוף ומחקר ומידת האנונימיזציה שבוצעה בהם לא הייתה מספקת ואפשרה זיהוי של חולים (Barth-Jones, 2012).

אמון. ערעור של הזכות לפרטיות מסכן גם את האמון שלקוחות רוכשים לארגון שבשירותיו הם משתמשים. לכן מבחינת הארגון יש חשיבות רבה לשקיפות בכל הנוגע לסוג הנתונים שנשמרים, היקפם והשימוש בהם, כמו גם אופן השמירה על הנתונים ואבטחתם. בכל פרסום על מקרה של פריצה למאגר נתונים של ארגון או חשיפה לגבי היקף הנתונים האישיים הנאספים ללא ידיעת הלקוחות, האמון של הלקוחות והמשתמשים נפגע. מצד אחד, התנהגות הצרכנים בהקשר הזה מעידה פעמים רבות על מה שמכונה "פרדוקס הפרטיות" - על אף שהצרכנים מעידים כי הפרטיות חשובה להם מאוד, הם מוסיפים לשתף מידע אישי ולעשות שימוש בכלים שאוספים מידע אישי רב. מצד שני, מחקרים מראים כי פגיעה ממושכת בפרטיות משפיעה לרעה על האמון של הלקוחות בארגון ועלולה להביא לעזיבה של לקוחות ולפגיעה בארגון (Shklovski, 2014). תופעה נוספת שפוגעת באמון היא ביצוע של ניסויים דיגיטליים. חברות רבות עושות שימוש בכלי הזה, המאפשר להן לבחון את היעילות של אספקטים שונים במוצר או בשירות שלהן. במסגרת ניסוי דיגיטלי, קבוצות של משתמשים בעלות מאפיינים שונים נחשפות שלא בידיעתן לגרסאות שונות של המוצר. במקרים מסוימים הניסויים חורגים מעבר לכך, למשל על ידי הצגת תוכן מוטה באתר, ועלולה להיות להם השפעה מזיקה על המשתמשים, שבכלל לא מודעים לכך שהם משתתפים בניסוי ולא נתנו את הסכמתם לכך (Kramer et al., 2014; Verma, 2014).

פתרונות לסוגיות האתיות ברובד מאגר הנתונים

כאמור, האתגר בעידן הביג דאטה הוא למצוא את האיזון הנכון בין הערך שארגונים יכולים להפיק מהמידע שהם מחזיקים לבין הסוגיות האתיות. במציאת האיזון יש לקחת בחשבון שיקולים של מידת הרגישות של הנתונים שנאספים והמשאבים שעומדים לרשות הארגון. נתחיל בפתרונות לבעיית הפרטיות.

מינימיזציה של המידע. הפתרון הראשון והפשוט ביותר הוא לצמצם מאוד את נפח הנתונים שהארגון מחזיק. הדבר מתאים בעיקר כאשר הארגון מסוגל להבין מראש מהי מטרת איסוף הנתונים והשימוש בהם, ויש לו יכולת לא לאסוף ולהחזיק נתונים מיותרים.

בהיעדר רצון לנקוט במינימיזציה, ישנו מגוון של **טכנולוגיות משמרות פרטיות:**

התממת נתונים (Anonymization או De-Identification). הוזכרה לעיל ועוסקת בהפיכת נתונים אישיים ומזוהים לנתונים אנונימיים. הכלי הזה רלוונטי בעת החזקת הנתונים לצורך אבטחתם, ובעת שיתוף והפצה של הנתונים לשם שמירה על פרטיות מושאי המידע. ראוי לציין כי אנונימיזציה מלאה באופן שלא ניתן יהיה לבצע זיהוי חוזר היא כמעט בלתי אפשרית. קיים מנעד רחב של שיטות התממה, החל מהסרת מזהים ישירים בלבד ועד שיטות הצפנה מתוחכמות. מידת ההשקעה של הארגון בתהליכי ההתממה תלויה במידת הרגישות של הנתונים ובמשאבים העומדים לרשותו (Finch, 2016).

הצפנה הומומורפית (Homomorphic Encryption). בעת איסוף וטיפול בנתונים רגישים, כגון נתונים רפואיים שונים, לעיתים נרצה שלא תהיה גישה לנתונים אפילו לגורם שמעבד ומנתח אותם. הצפנה הומומורפית מאפשרת לניתוחים ולחישובים מסוגים מסוימים להתבצע על נתונים מוצפנים בלי להידרש לנתונים הגולמיים. הצפנה זו שימושית בעיקר ביישומים שהמידע בהם רגיש, כגון בריאות או פיננסים (Kaufman, 2020).

פרטיות דיפרנציאלית (Differential Privacy). זוהי למעשה הגדרה מתמטית של מושג הפרטיות, המכמתת את ההסתברות שפרט מסוים נכלל במאגר נתונים. השיטה מתבססת על הוספת רעש סטטיסטי לנתונים בטרם ניתוחם, כך שכל תשאול שלהם לא יאפשר זיהוי של פרטים ספציפיים. השימוש בשיטה זו דורש מציאת איזון בין מידת הפרטיות הנדרשת ומידת הדיוק של הנתונים, ויכול להתאים במקרים של צורך בשיתוף נתונים, פתיחתם לציבור וניתוח של נתונים אישיים רגישים. לדוגמה, שימוש בשיטת הפרטיות הדיפרנציאלית מבוצע ברשות האוכלוסין האמריקאית (Hawes, 2020).

מעבר לטכנולוגיות שפורטו לעיל, שמטרתן לטפל בנתונים שכבר נאספו, קיימת גישה של **הנדסת פרטיות** (Privacy by design) הרלוונטית בעת תכנון של מערכות חדשות. הגישה הזו היא למעשה מסגרת לחשיבה ותכנון, ודוגלת בכך שהפונקציונליות של המערכת והפרטיות של המשתמשים אינן מייצרות משחק סכום אפס ואינן באות זו על חשבון זו, אלא שבתכנון נכון של המערכת מייצרות סכום חיובי. בהתאם לגישה זו יש לתכנן את המערכת מראש כך שהפרטיות תהווה את ברירת המחדל ולא תדרוש מהארגון השקעת משאבים רבים בהמשך לצורך פתרון בעיות וכיבוי שרפות בדיעבד (Cavoukian, 2013).

אפליקציית "המגן" שפותחה במשרד הבריאות במסגרת המאבק בקורונה, היא דוגמה למערכת שנבנתה ועוצבה על פי עקרונות גישת הנדסת הפרטיות. המערכת מאפשרת לאתר מגעים ולהתריע בפני מי שאמורים להיכנס לבידוד, ועושה זאת בלי לאסוף את נתוני המיקום האישיים שלנו במקום מרכזי, אלא משאירה אותם באפליקציה בטלפון בלבד. המצדדים באפליקציית המגן מדגישים את החשיבות של השימוש באפליקציה ככלי בלעדי (ללא שימוש מקביל באיכונים סלולריים על ידי שירות הביטחון) כדי להגביר את אמון הציבור באפליקציה, מה שירחיב את השימוש בה וייתר את השימוש באמצעי הפוגעני יותר של האיכון (אלטשולר-שוורץ ואריאלי, 2020). ההיענות הנמוכה מצד הציבור לשימוש באפליקציה עשויה להעיד על רמת אמון נמוכה של הציבור במדינה, שהעבירה במקביל חוק למעקבים סלולריים.

פתרון לבעיית האמון ניתן למצוא בקביעת מדיניות ארגונית ברורה ושקופה בנוגע לתהליכי איסוף הנתונים, החזקתם, אבטחתם והשימוש בהם. סקר בין-לאומי שנערך בקרב עובדים בארגונים גדולים הראה כי רובם מאמינים שלמדיניות הארגון בתחומי השמירה על הפרטיות של הלקוחות ואבטחת המידע שלהם יש השפעה ניכרת על אמון הלקוחות בחברה. לפיכך, יישום של מדיניות ברורה בתחום יכול גם לבדל את המוצר או השירות של הארגון ולחזק את היתרון התחרותי שלו (Schlesinger, 2017). עוד נמצא כי חברות כאלה גם זוכות לאמון מצד המשקיעים, דבר שבא לביטוי במחיר המניה (Martin et al., 2018).

רגולציה. הרגולציה הקיימת והמתהווה בנושא, בארץ ובעולם, מתייחסת בעיקר לאיסוף והחזקה של מידע אישי. מטרתה איננה שמירה על הפרטיות באופן ישיר, אלא הגדרת קווים מנחים לתהליכי האיסוף, ההחזקה, השיתוף והניתוח של מידע אישי. העקרונות המרכזיים של הרגולציה בארץ (חוק הגנת הפרטיות, 1981 והתקנות הנלוות), באירופה (GDPR, 2016) ובמקומות אחרים (כגון התקנות בקליפורניה, CCPA, 2018) הם יידוע המשתמשים בדבר איסוף הנתונים ומטרתו, קבלת הסכמה מהמשתמשים לאיסוף המידע והסכמה להעברה או מכירה של נתונים אישיים, צמידות המטרה (שימוש בנתונים רק לצורך לשמו נאספו ומחיקתם בתום תקופת השימוש) ומתן גישה לפרט לנתונים שלו. האתגר העומד בפני הרגולציה בתחום הוא עצום מכיוון שהטכנולוגיה והתעשייה מתקדמות בקצב מהיר מאוד כל העת, והרגולציה עלולה למצוא את עצמה מטפלת בבעיות האתמול במקום בבעיות המחר.

רובד II – ניתוח הנתונים

הרובד השני של השימוש בביג דאטה כולל את כל התהליכים והשיטות שניתן להפעיל כדי להפיק תועלת מן הנתונים שנאספו, לזהות מאפיינים של לקוחות, להפיק תובנות לגבי דרכי פעולה ולקבל החלטות מבוססות ניתוח. אלה פעולות שמתבצעות בתוך הארגון או מחוצה לו במסגרת מיקור חוץ. הרובד הזה כולל ניתוח של הנתונים בכלים שונים, החל משיטות פשוטות המיושמות על ידי עובדים אנושיים, ועד להפעלת אלגוריתמים מתוחכמים ובינה מלאכותית. כרקע לדיון בסוגיות האתיות ברובד זה, חשוב ליצור תחילה מכנה משותף בסיסי להכרת המושגים הרלוונטיים והטכנולוגיות הרלוונטיות:

בינה מלאכותית (Artificial Intelligence – AI): מושג המתייחס לכלל הטכניקות המאפשרות למחשבים לחקות התנהגות אנושית. טרום עידן הביג דאטה, הבינה המלאכותית הייתה בעיקרה מבוססת חוקים (Rule-based), ואילו כיום היא משתמשת בביג דאטה ובטכניקות של למידת מכונה. כלי ה-AI מאפשרים לנתח את הנתונים הנאספים, לזהות בהם דפוסים ולערוך תחזיות (מה ההסתברות שמשתמש יתעניין ברכישת מוצר מסוים),

לבצע קלסיפיקציות (למשל, זיהוי עצמים בתמונות, או סיווג לקוחות) ולאפשר קבלת החלטות אלגוריתמית (למשל, האם לאשר ללקוח מסגרת אשראי).

למידת מכונה (Machine Learning – ML): תת-תחום של בינה מלאכותית המתבסס על נתונים ועושה שימוש בטכניקות כמותיות מתוחכמות כדי לאפשר למחשבים (או "מכונות") לבצע משימות ולקבל החלטות, וכן להשתפר בביצוע פעולות, בהתבסס על ניסיון. אלגוריתמים של למידת מכונה המסתמכים על היקפים גדולים של דאטה ומאפשרים לתוכנה להתאמן בביצוע משימות, כוללים רשתות נוירונים (Neural Networks) ולמידה עמוקה (Deep Learning).

המשך הניתוח כאן יתייחס בעיקר לניתוח נתונים מבוסס בינה מלאכותית. עם זאת, חשוב לציין כי בעיות יכולות להתעורר לאורך כל הספקטרום גם בשיטות הפשוטות וגם במתוחכמות. עוד כדאי לזכור כי גם כאשר פועלים כלי ניתוח ממוחשבים ו"אוטונומיים", יש הרבה החלטות אנושיות שמכוונות את התהליך ומשפיעות על תוצאותיו.

סוגיות אתיות ברובד ניתוח הנתונים

מערכות בינה מלאכותית נועדו לטייב את קבלת ההחלטות, לייעל את התהליכים ולקצרם, וגם להפוך אותם למוטים פחות, מפני שכך הם יהיו פחות מושפעים מטעויות אנוש, מהטיות אנושיות ומדעות קדומות. בפועל, אנחנו נתקלים במקרים לא מעטים שבהם מתרחשות טעויות, הטיות ואפליה גם במערכות הללו. ייתכן שחלק מן הכשלים הללו מקורם בחוסר בשלות של המערכות. בכל אופן התעשייה נעה קדימה במהירות והמערכות הללו חודרות ליותר ויותר תחומים ומקבלות החלטות שמשפיעות על הרבה מאוד אנשים. הסוגיות האתיות המהותיות ברובד ניתוח הנתונים הן חוסר דיוק והטיות, וכן שימוש בנתונים לצורך השפעה ושינוי התנהגות.

חוסר דיוק והטיות. הספר "נשק להשמדה מתמטית" (O'Neil, 2016) מתאר כיצד השימוש באלגוריתמים לצורך קבלת החלטות גורם לאפליה של אוכלוסיות חלשות במגוון רחב של תחומים, כגון חינוך, תעסוקה ופרסום. לטענת המחברת, השילוב של שימוש נרחב באלגוריתמים (למשל כאשר הם משמשים בחברות כוח אדם רבות לצורך סינון מועמדים לעבודה), יחד עם היותם "סודיים" (כלומר דרך קבלת ההחלטות באמצעותם איננה שקופה ונגישה), הופך את האלגוריתמים הללו למסוכנים.

הגורמים להטיות מגוונים, וכוללים בין היתר שימוש בנתונים שאינם מייצגים אוכלוסיות שונות, או בנתונים שכוללים אפליה היסטורית, שימוש במשתנים שיש להם קורלציה למשתנים מפלים, והגדרה לא מתאימה של המדדים ל"הצלחה" של אלגוריתמים מסווגים (d'Alessandro et al., 2017). ניתן לזהות את הגורמים הללו בכמה מהדוגמאות שעוררו הדים בתקופה האחרונה:

מערכת המשפט: מערכת ה-COMPAS מיושמת במערכת המשפט במדינות שונות בארה"ב. מטרתה היא לסייע לשופט להכריע אם לשחרר עצורים בערבות, ומה יהיה משך מאסרם של מורשעים. המערכת, שעושה שימוש בכלי בינה מלאכותית ומתבססת על נתונים מגוונים לגבי העצורים וכן על נתונים היסטוריים מקיפים, קובעת את דרגת המסוכנות של העצירים מ-1 עד 10, כאשר למעשה מדובר בהסתברות שנותנת המערכת לאפשרות שהם יבצעו עבירות נוספות בעתיד. הכנסת מערכות אוטומטיות מסוג זה למערכת המשפט האמריקאית נבעה בין היתר מהדרישה למנוע אפליה נגד מיעוטים ומטענות על גזענות בקרב שופטים. אולם מספר מחקרים שבוצעו לאחר כמה שנים שבהן המערכת יושמה, מצאו כי במקרים רבים דווקא המערכת נוטה להחמיר עם אוכלוסיות מיעוטים (Angwin et al., 2016; Dressel and Farid, 2018). ממצאים אלה העלו שאלות בנוגע למידת הגינותה של המערכת, אך החברה שמפתחת את מערכת הדירוג הזו הצהירה שאינה משתמשת במשתני גזע או מוצא, אלא בתוצאות שאלון נרחב שעליו משיב העצור וכן ברקורד הפלילי שלו.

איור מס' 2 ממחיש את הסוגיה באמצעות שני מקרים הלקוחים מתוך תחקיר על מערכת ה- COMPAS (Angwin et al., 2016). לשני האנשים המופיעים באיור יש בעברם אירוע פלילי אחד. האדם משמאל הוא לבן וסווג על ידי המערכת כבעל סיכון נמוך, אולם לאחר האירוע המתועד הוא נעצר שלוש פעמים נוספות בשל אחזקת סם. לעומתו, האדם הימני הוא שחור וסווג כבעל סיכון גבוה, אך לאחר האירוע לא ביצע אף עבירה נוספת.

איור 2: פרופיל העצורים מתוך תחקיר ProPublica

קבלה לעבודה: אלגוריתמים משמשים חברות לצורך סינון קורות חיים של מועמדים לעבודה וייעול וטיוב של תהליך הגיוס של העובדים. גם בתחום זה אחת המטרות של השימוש במערכות הללו היא למנוע אפליה ולהגן על התהליך מפני דעות קדומות. אולם גם כאן, כפי שהתברר במגוון מקרים, השימוש באלגוריתמים לא מונע את ההטיות. בין היתר נמצאה הטיה במערכת למיון וגיוס שפותחה בחברת אמזון, והמערכת נגנזה לפני שיושמה (Dastin, 2018). אחת הבעיות במערכות הללו היא שהן מתבססות על למידה מנתונים היסטוריים, ולעיתים מזומנות הנתונים ההיסטוריים משקפים אפליית נשים. בנוסף, גם כאשר המגדר אינו חלק מהנתונים המוזנים למערכת, המערכת מצליחה לאתר אותו באופן עקיף, למשל מתוך קורות חיים הכוללים חברות במועדוני נשים בספורט (Mann and O'Neil, 2016).

תופעה דומה מתרחשת גם בקביעת מסגרות אשראי. לדוגמה, בהשקת כרטיס האשראי של חברת אפל התפרסמו מספר מקרים שהצביעו על הטיה בקביעת מסגרת האשראי לטובת לקוחות גברים, שקיבלו מסגרת אשראי גבוהה עד פי 10 מזו שניתנה לנשותיהם גם במקרים שבהם כל הנתונים הפיננסיים של בני הזוג דומים מאוד (Knight, 2019). החברה הצהירה שלא השתמשה במשתנה המגדר כחלק מהמודל שלה, אולם סביר להניח שבחירת המשתנים או הדאטה במודל אפשרו להטיה המגדרית לחלחל לתוכו.

זיהוי פנים. הטכנולוגיה של זיהוי פנים עושה שימוש בלמידת מאגרי תמונות, ומאפשרת לזהות בני אדם ללא צורך באמצעי זיהוי חיצוניים כגון תעודת זהות, דרכון או טביעת אצבע. למעשה, באמצעות טכנולוגיות זיהוי פנים ניתן לזהות אנשים גם ללא ידיעתם. במספר שדות תעופה בעולם משתמשים בטכנולוגיות לזיהוי פנים, וגם המשטרה מגבירה את השימוש בכלי הזה כדי לאתר פושעים. בסין ניתן גם לבצע פעולות שונות, כגון תשלום, באמצעות זיהוי פנים.

סוגיה אתית שעולה כתוצאה מהשימוש בטכנולוגית זיהוי פנים היא הדיוק בזיהוי. מזה כשני עשורים משתמשים במשטרה במערכות כאלו. מחקרים מראים כי הטכנולוגיות הללו עובדות טוב יחסית כשמדובר באנשים לבנים, אך בקרב שחורים שיעור הטעויות גבוה יחסית. ביוני 2020 בוצע בארצות הברית מעצר שגוי ראשון, כאשר אזרח נעצר בטעות בחשד לביצוע שוד בשל התאמה שגויה של אלגוריתם לזיהוי פנים. מדובר היה באדם אפרו-אמריקני, והמקרה עורר מחדש את הוויכוח המתנהל לגבי השימוש בטכנולוגיות אלה על ידי כוחות הביטחון (Hill, 2020). מקור הטעויות נובע ככל הנראה מייצוג חסר או יתר של אוכלוסיות שונות במאגרי התצלומים שבעזרתם אומנו המערכות (Buolamwini and Gebru, 2018; Snow, 2018). דוגמאות דומות קיימות גם במערכת הבריאות ובענף הביטוח.

השפעה ושינוי התנהגות (Behavior Modification). אחד השימושים המרכזיים בנתונים האישיים הנאספים אודות משתמשים, בעיקר ברשתות החברתיות, הוא הניתוח שלהם לצורך השפעה על התנהגות – שהייה ממושכת יותר באתר, רכישה של מוצרים וכדומה. למעשה נמצא שהניתוח של מאפייני המשתמש יכול להביא גם לשינוי התנהגות מחוץ לגבולות האתר או המסך, כגון יציאה להשתתפות בהפגנות או בבחירות. היכולת להשפיע על אנשים על סמך נתונים אישיים רבים שלהם שנאספים ומנותחים ללא ידיעתם, מביאה לטענת המבקרים לקיטוב בחברה ולפגיעה בדמוקרטיה (Zuboff, 2019; Shmueli, 2020).

הכלים שתוארו לעיל משמשים ארגונים עסקיים וכן מדינות וגורמי שיטור ואכיפה. הכוח הרב שטמון בשילוב של כלי בינה מלאכותית יחד עם מאגרי נתונים רחבי היקף הוא סיבה לדאגה במקרה של שימוש לרעה בנתונים. בהיעדר כללים ברורים בידי מי נמצאת הטכנולוגיה, למי מותר

להשתמש בה ותחת אילו תנאים, ישנה סכנה ברורה לפרטיות וגם לביטחון של האזרחים. למשל, ערים רבות מרושתות במצלמות כדי שיוכלו לנהל באופן יעיל את משאבי העיר. לא היינו רוצים שתצלומי הפנים שנקלטים בהן יזוהו ויתאפשר מעקב אחרינו ברחבי העיר, מכיוון שבידיים הלא נכונות הדבר עלול להיות מסוכן. חשש זה הביא להתנערות של חברות משיתופי פעולה עם משטרות וממשלות, וגם למחאות מבפנים מצד עובדים בחברות טכנולוגיה שמייצרות שיתופי פעולה כאלה (Kelly, 2019).

פתרונות לסוגיות האתיות ברובד ניתוח הנתונים

קיים מגוון רחב של כלים שארגונים יכולים ליישם במענה לסוגיות האתיות ברובד זה, ובכללם הגברת המודעות וביצוע הכשרות, יישום כלים טכנולוגיים ורגולציה.

הגברת מודעות. אנחנו מניחים שכלי בינה מלאכותית הם מדעיים, ולכן הם מטבעם אובייקטיביים, אינם מוטים ואינם יכולים לטעות. ההנחה הזו אינה נכונה, מכיוון שהחלטות אנושיות וסובייקטיביות בתהליכי איסוף הנתונים ובניית האלגוריתמים ישפיעו על התוצאות שלהם. לכן נדרשת מודעות לנושא הזה, וכן נקיטת צעדים לאורך התהליך כדי לצמצם את ההטיות והטעויות של תהליכי הבינה המלאכותית.

הכשרת מדעני הנתונים. ניתן לבצע הכשרות שבהן ייחשפו מדעני הנתונים לבעיות וגם ילמדו כיצד ניתן למנוע או לצמצם את האפליה באלגוריתמים שהם מפתחים. בין השאר ההכשרה תכלול התייחסות לדאטה, לתיוג שלו, להגדרת ההצלחה, לבחירת המשתנים ולבחירת מאפיינים ופרמטרים שונים של המודל (d'Alessandro et al., 2017). בתי ספר למדעי המחשב במדינות רבות כבר הוסיפו הכשרות מעין אלה לתוכנית הלימודים.

טיוב הנתונים ובקרה. כלי בינה מלאכותית מסוגלים להפיק תובנות מנתונים ולקבל החלטות בצורה אלגוריתמית, אך הם אינם יכולים להיות טובים יותר מהנתונים עצמם. מקרים בהם הנתונים חסרים, אינם מייצגים אוכלוסיות שונות, טומנים בחובם אפליה היסטורית, או פשוט אינם מדויקים, כל אלה עלולים לייצר תוצאות בעייתיות. לכן לפני המעבר לתהליכי עיבוד הנתונים רצוי להקדיש מאמץ רב ככל האפשר לטיוב הנתונים הגולמיים. כיום קיימים שורה של כלים טכנולוגיים שאמורים לסייע בתהליכי טיוב הנתונים ופיתוח האלגוריתמים (Lomas, 2018). לצד כלים אלו ישנן חברות שנותנות "תו תקן" לאחר שהן בודקות כי בנתונים שנאספו ובאלגוריתמים שפותחו אין אפליות של אוכלוסיות שונות. (Hempel, 2018)

רגולציה. ביקורת על "הקופסה השחורה" ודרישה לחייב ארגונים לספק הסבר על האופן שבו התקבלו ההחלטות מתחילות לעלות גם מצד רגולטורים. הרגולציה במקומות שונים דורשת מניעת אפליה בניתוח נתונים ומתן אפשרות לפרט לדרוש שלא יתקבלו לגביו החלטות על ידי אלגוריתמים אוטונומיים שלא ניתן להסביר. הרגולציה צפויה להתרחב, ובעתיד ארגונים יצטרכו לעמוד גם בכללים ובאסדרות כמו בתחום דיני ההגנה על המידע האישי (Buiten, 2019).

סיכום

ההתקדמות המואצת בכל הנוגע לשימוש בביג דאטה ובטכנולוגיות המסתמכות על ביג דאטה, מביאה עימה גם שורה של בעיות ושאלות אתיות. מאמר זה סקר את העיקריות שבהן, וגם את הכלים הטכנולוגיים והתהליכים הארגוניים שעומדים לרשות ארגונים לצורך התמודדות עם הבעיות והשאלות הללו.

מכיוון שאין מסגרת אתית ברורה לפיתוח הכלים והשימוש בהם, אחריות רבה מוטלת על הארגונים שצריכים לפעול באחריות ובשיקול דעת. על הארגון להכיר את הבעיות שנובעות מאיסוף נתונים מקיף אודות משתמשים ולקוחות, ללמוד כיצד להתמודד איתן ולאזן בין האינטרסים השונים. איור מס' 3 מסכם את השלבים, את הסוגיות האתיות ואת הבעיות שמתעוררות בשני רובדי השימוש בטכנולוגיות ביג דאטה, וכן את הכלים שהארגון יכול לאמץ כדי להתמודד עם בעיות אלו:

איור מס' 3: סיכום השלבים, הסוגיות האתיות, הבעיות והכלים לפתרון

רובד 1 מאגר הנתונים		רובד 2 ניתוח הנתונים
איסוף נתונים החזקה ואבטחה שיתוף והפצה	שלבים	ניתוח והפקת תובנות קבלת החלטות מבוססת בינה מלאכותית
פרטיות אמון	סוגיות אתיות	דיוק הניתוחים גישה לנתונים ולכלים
פגיעה בזכות לפרטיות פגיעה באמון הלקוחות	בעיות	הטיות ואפליית אוכלוסיות שימוש לרעה בכלים רבי עוצמה
התממה (ספקטרום רחב) הנדסת פרטיות מדיניות ארגונית רגולציה	כלים לפתרון	מודעות והכשרה טיוב הדאטה כלי בקרה רגולציה

ארגון שיכיר היטב את הסוגיות האתיות שנובעות מיישום טכנולוגיות ביג דאטה, יטפל באופן נאות במאגר הנתונים שלו, וידע להתנהל באופן שמצמצם את הפגיעה בפרטיות ואת החשש לקבלת החלטות מוטה, יפיק מכך תועלת עסקית רבה. התועלת הישירה היא עמידה בדרישות רגולציה שמטפלת באופן חלקי בסוגיות שהזכרנו במאמר זה, אך התועלת המשמעותית יותר תנבע מחיזוק האמון בין הארגון לבין לקוחותיו והמשתמשים בשירותיו.

ד"ר אהרונה פפר pfeffer@tauex.tau.ac.il

רשימת מקורות

Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research* 81, 1-15.

California Consumer Privacy Act of 2018 (CCPA), *State of California, Department of Justice*.

Cavoukian, A. (2013). Privacy by Design: Leadership, Methods, and Results. In: Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds) *European Data Protection: Coming of Age*. Springer, Dordrecht.

Dastin, J. (2018), Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women. *Reuters*. October 11 2018, Retrieved from https://www.reuters.com

Douriez, M., Doraiswamy, H., Freire, J. and Silva C. (2016). Anonymizing NYC Taxi Data: Does It Matter? *Proceedings - 3rd IEEE International Conference on Data Science and Advanced Analytics, DSAA 2016*, 140-148.

Dressel, J., and Farid H. (2018). The Accuracy, Fairness, and Limits of Predicting Recidivism. *Science Advances,* 4(1) eaao5580.

Duality dualitytech.com/

Finch, K. (2016), A Visual Guide to Practical Data De-Identification. *Future of Privacy Forum*. April 25, 2016

Gebhart, G. (2018). Facebook, This Is Not What "Complete User Control" Looks Like. *Electronic Frontier Foundation*. April 11, 2018.

אלטשולר-שוורץ, ת. ואריאל ר. (2020). מעקבים דיגיטליים בחסות הקורונה - חלופות למעקבי השב"כ. *חוות דעת המכון הישראלי לדמוקרטיה*, 24 יוני 2020.

בירנהק, מ. (2018) "הגנה על הפרטיות בעיר הדיגיטלית", בתוך: טלי חתוקה (עורכת) "העיר בעידן הדיגיטלי", *אוניברסיטת תל אביב*.

"חוק הגנת הפרטיות", התשמ"א 1981.

"תוכנית לאומית לקידום תחום הבריאות הדיגיטלית כאמצעי לשיפור הבריאות וכמנוע צמיחה", החלטת ממשלה 3709, מרץ 2018.

תקנות זכויות החולה (שימוש מחקרי במידע בריאות), משרד הבריאות, 2019.

"General Data Protection Regulation" GDPR (2016), *The European Parliament and Council of the European Union*.

Hawes, M.B. (2020). Implementing Differential Privacy: Seven Lessons from the 2020 United States Census. *Harvard Data Science Review*. https://doi.org/10.1162/99608f92.353c6f99

Hempel, J. (2018). Want to Prove Your Business Is Fair? Audit Your Algorithm. *Wired Magazine*. May 9, 2018. Retrieved from https://www.wired.com/

Hill, K. (2020). Wrongfully Accused by an Algorithm. *The New York Times*, June 24 2020, Retrieved from https://www.nytimes.com/

Kaufman, A. (2020). Privacy-Preserving Information Sharing Against Financial Crime. *Dualitytech.com blog*. May 18, 2020.

Kelly, M. (2019), Google, Amazon, and Microsoft face New Pressure Over Facial Recognition Contracts. *The Verge.* , January 15, 2019. Retrieved from https://www.theverge.com/

Knight, W. (2019). The Apple Card Didn't 'See' Gender—and That's the Problem. *Wired Magazine*, November 11, 2019.

Kramer, A.D., Guillory, J.E. and Hancock, J.T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788-8790.

Lomas, N. (2018). Accenture Wants to Beat Unfair AI With a Professional Toolkit. *TechCrunch*. June 9, 2018. Retrieved from https://techcrunch.com/.

Lynskey, D. (2019). 'Alexa, Are You Invading my Privacy?' – The Dark Side of Our Voice Assistants. *The Guardian*. October 9, 2019. Retrieved from https://www.theguardian.com

Mann, G. and O'Neil, K. (2016). Hiring Algorithms Are Not Neutral. *Harvard Business Review*, December 9, 2016.

Martin, K., Borah, D., and Palmatier, R.W. (2018). Research: A Strong Privacy Policy Can Save Your Company Millions. *Harvard Business Review*. February 15, 2018.

Mason, R.O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, 10(1), 5-12.

de Montjoye, Y., Hidalgo, C., Verleysen, M. and Bondel V.D. (2013). Unique in the Crowd: The Privacy Bounds of Human Mobility. *Nature Scientific Reports*, *3*, 1376.

Nakashima, R. (2018). Google Tracks Your Movements, Like it or Not. *AP*. August 14, 2018. Retrieved from https://apnews.com

Narayanan, A. and Shmatikov V. (2008). Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy*, 111-125.

O'Neil, K. (2016). *Weapons of Math Destruction*. Crown Books.

Schlesinger, S. (2017). Digital Dilemma: Turning Data Security and Privacy Concerns into Opportunities. *Harvard Business Review Analytic Services*.

Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H. and Borgthorsson H., (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile. *CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2347–2356.

Shmueli, G. (2020). "Improving" Prediction of Human Behavior Using Behavior Modification (https://arxiv.org/pdf/2008.12138.pdf).

Snow, J. (2018). Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots. *American Civil Liberties Union, July 26, 2018*

Thompson, S.A., and Warzel C., (2019). One Nation, Tracked: An Investigation into the Smartphone Tracking Industry. *The New York Times Opinion*. December 19, 2019, Retrieved from https://www.nytimes.com/.

Valentino-DeVries J., Singer N., Keller M.H. and Krolik A. (2018). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. *New York Times*. December 10, 2018. Retrieved from https://www.nytimes.com/

Verma I.M., (2014). Editorial Expression of Concern: Experimental Evidence of Massive Scale Emotional Contagion Through Social Networks. *Proceedings of the National Academy of Sciences*, 111(24), 10779.

Zuboff S., (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *PublicAffairs*.