

## כשהדירקטור נכנס לאטרף מכיוון שפרצו לך למאגר המידע / אסנת נתאי, עו"ד\*

באוקטובר 2021 בוצעה פריצה למספר מאגרי מידע ישראלים, כאשר המוכר מבניהם היה מאגר המידע של תוכנת ההיכריות לקהילה הגאה, אטרף (המקבילה הישראלית לגריינדר, שתפס את מקומה עם קריסתה). ברגע אחד נחשף מידע אישי רגיש ביותר (לרבות פרטים חסויים ביותר, תמונות עירום, ועוד), ומשתמשים רבים (לרבות כאלה שטרם יצאו מהארון) נכנסו לאטרף (תרתי משמע), מהפחד שזהותם או פרטיהם ייחשפו. הפרשה הסתיימה לבסוף בחקירה מטעם הרשות להגנת הפרטיות בחשד של התרשלות באבטחת המידע אשר לא ידוע כיצד הסתיימה.

שנתיים וחצי לאחר מכן, בתחילת 2024, אפליקציית אטרף חזרה לחיים, וכמעט במקביל אליה גם הועבר תיקון 13 לחוק הגנת הפרטיות<sup>1</sup> שהוראותיו נכנסות לתוקף בחודש אוגוסט, 2025, והוא מעדכן ומבהיר את החקיקה בתחום, תוך קביעת הסדרים חדשים ומתקדמים, והקניית כלי אכיפה יעילים בהתאמה לאתגרי העידן הדיגיטלי, מתוך כוונה להגביר את ההגנה על זכות היסוד לפרטיות וחיוק ההתמודדות מול איומי הסייבר. התיקון מטיל אחריות על חברות בתחום שמירת הפרטיות והגברת הפיקוח על החזקה וסחר במאגרי מידע תוך הטלת עיצומים כספיים גבוהים במצב של הפרה והחוק גם יוצר אחריות אישית של דירקטורים ונושאי משרה. משמעות הדבר היא, שבחברה שאינה מקפידה בנושא הגנת הפרטיות של לקוחותיה עשויים דירקטורים ונושאי משרה להיות אחראים באופן אישי גם במישור האזרחי וגם במישור הפלילי.

התיקון גם מתקן עיוות היסטורי בחוק, שדרש בפועל כמעט מכל עסק קטן להחזיק ברישיון מאגר מידע (דרישה שבפועל כלל לא ניתנת הייתה לאכיפה). לאחר התיקון אין עוד צורך לרשום את מאגרי המידע הקטנים שבניהול עסקים, למעט מאגרים המנוהלים מתוך כוונה של סחר במידע. התיקון מעדכן ומדייק גם את השאלה של מה נחשב ל"מידע בעל רגישות מיוחדת", אשר לגביו קיימת חובת הודעה מפורטת לרשות לכל גודל מאגר, והכל תוך התאמה לסטנדרטים הבינלאומיים, לרבות רגולציית הגנת המידע של האיחוד האירופי (GDPR).

למרות שהחוק כיום לא קובע במפורש את זהות האורגן האמור לפקח על יישום הדרישות, נייר עמדה של הרשות להגנת הפרטיות מחודש ינואר 2024,<sup>2</sup> קובע חובות מפורטות שהן באחריות דירקטוריון החברה ודורש מחברי הדירקטוריון לא רק להיות מעורבים בפיקוח והבקרה בתחום הגנת המידע אלא גם להעביר נוהל אבטחת המידע, לבצע סקרי סיכונים ולוודא שהמידע מוגן. עמדה זו של הרשות יוצרת בפועל סטנדרט זהירות לדירקטורים וחושפת את הדירקטורים לאחריות אישית באופן דומה לזה שנפסק, למשל, כבר ב-1996 בבית המשפט של דלאוור, ארה"ב<sup>3</sup>, שם בעלי מניות של חברת Caremark הגישו תביעה נגזרת נגד דירקטורים בטענה שלא הציבו מערכות בקרה פנימיות נאותות. באותו מקרה, בית המשפט האמריקאי קבע שחובת דירקטוריון החברה לדאוג להטמעת מערכות בקרה ושליטה לגבי ציות לתקנות הרגולטוריות ולפקח והפרת החובה תקים אחריות.

לאור האמור, חשוב ביותר בכל חברה המחזיקה מאגר מידע, כי יועבר נוהל אבטחת מידע מסודר ותכנית אכיפה פנימית אשר לא רק יוודאו את ההגנה על המידע אלא גם יגנו על דירקטורים ונושאי משרה במקרה של סיכון למידע. חשוב מאוד שנוהל כזה ותכנית האכיפה הפנימית ייבנו בשיתוף עם יועצים משפטיים בעלי הכרות עמוקה של התחום, אשר יהיו מעורבים גם בהליכי יישום התכנית ואכיפתה.

\* עו"ד אסנת נתאי הינה חלק מצוות משרד אפיק ושות' ([www.afiklaw.com](http://www.afiklaw.com)). עו"ד נתאי בוגרת הפקולטה למדעי החברה באוניברסיטה העברית בירושלים ובוגרת תואר במשפטים, בעלת תעודת גישור במשפחה מטעם מרכז גבים. אין בסקירה כללית זו משום ייעוץ משפטי כלשהו ומומלץ להיוועץ בעורך דין המתמחה בתחום זה בטרם קבלת כל החלטה בנושאים המתוארים בסקירה זו. לפרטים נוספים: 03-6093609, או באמצעות הדואר האלקטרוני: [afiklaw@afiklaw.com](mailto:afiklaw@afiklaw.com)

<sup>1</sup> "חוק הגנת הפרטיות, תשמ"א-1981" (תיקון מס' 13) תשפ"ד-2024, ס"ח תשפ"ד 3287, 1430

<sup>2</sup> הנחיית הרשות להגנת הפרטיות מס' 1/2024 - [https://www.gov.il/he/pages/the\\_board\\_role](https://www.gov.il/he/pages/the_board_role)

<sup>3</sup> 2d 959 (Del Ch. 1996) Caremark International Inc. Derivative Litigation, 698 A

## **When a Director “Enters an Atraf State” (Goes Frenzy) Because of a Data Breach/ Osnat Nitay, Adv.\***

In October 2021, a number of Israeli databases were hacked, the best known of which was the database of the gay dating app, Atraf (the Israeli equivalent of Grindr, which took its place when it collapsed). In one moment, highly sensitive personal information was revealed (including highly confidential details, nude photos, and more), and many users (including those who have not yet come out of the closet) went into a literal state of “Atraf” (the Israeli slang word for “frenzy”), for fear that their identity or details would be revealed. The affair finally ended in an investigation by the Israeli Privacy Authority for suspicion of negligence, the result of which is unknown.

Two and a half years later, at the beginning of 2024, the Atraf application came back to life, and almost at the same time, Amendment 13 to the Israeli Privacy Protection Law was passed, which provisions enter into force in August, 2025, and it updates and clarifies the legislation in the field. The amendment establishes new and advanced arrangements and provides effective enforcement tools in line with the challenges of the digital age, with the intention of increasing the protection of the fundamental right to privacy and strengthening the fight against cyber threats. It imposes liability on corporations in the field of privacy protection and increases supervision on possession and trade in databases while imposing high financial sanctions in the event of a violations. It also creates personal liability for directors and officers. This means that if a corporation does not take care to protect the privacy of its customers, its directors and officers may be personally liable both on the civil and criminal levels.

The amendment also corrects a historical distortion in the law, which in practice required almost any small business to hold a database license (a requirement that in practice could not be enforced at all). After the amendment, it is no longer necessary to register small databases, with the exception of databases intended for trading information. It also updates and clarifies the question of what is considered "sensitive data", for which there is a reporting obligation for any size of database, all while conforming to international standards, including the EU Data Protection Regulation (GDPR).

Although the law currently does not explicitly determine the identity of the corporate body to supervise the implementation of the requirements, a position paper of the Israeli Privacy Authority dated January, 2024, establishes detailed obligations that are the responsibility of the board of directors and requires the members of the board of directors not only to be involved in supervision and control but also to pass the information security procedures, perform risk surveys and ensure that data is protected. This creates a standard of care and exposes directors to personal liability in a manner similar to what was decided, for example, already in 1996 in the Court of Delaware, USA\*\*, where shareholders of the Caremark company filed a derivative suit against directors on the grounds that they did not put in place adequate internal controls. In that case, the American Court held that the company's board of directors breached the duty to implement control systems and to monitor it.

In light of the above, it is extremely important for any company that maintains a database to create proper procedures and an internal enforcement plan which will not only ensure the protection of data but also protect directors and officers in the event of a risk to the information. It is very important that such a procedure and the internal enforcement plan be built in collaboration with legal advisors with deep knowledge of the field, who will also be involved in the procedures for implementing the plan and enforcing it.

---

\***Osnat Nitay, Adv.** is part of the legal team of Afik & Co. ([www.afiklaw.com](http://www.afiklaw.com)). Mrs. Nitay is a graduate of the Faculty of Social Sciences at the Hebrew University of Jerusalem and has a degree in law. She holds a family mediation certificate from the Gevim Center. This overview does not constitute any legal advice and it is recommended to consult a lawyer who specializes in this field before making any decision on the issues described in this overview. For more details: 03-6093609, or by e-mail: [afiklaw@afiklaw.com](mailto:afiklaw@afiklaw.com)

\*\*Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del Ch. 1996)

## **Cuando un director “entra en estado de Atraf” (se vuelve frenético) debido a una filtración de datos / Osnat Nitay, Abogada.\***

En octubre de 2021, varias bases de datos israelíes fueron hackeadas, la más conocida de las cuales fue la base de datos de la aplicación de citas gay, Atraf (el equivalente israelí de Grindr, que ocupó su lugar cuando colapsó). En un momento, se reveló información personal altamente sensible (incluidos detalles altamente confidenciales, fotos de desnudos y más), y muchos usuarios (incluidos los que aún no han salido del armario) entraron en un estado literal de “Atraf” (la palabra del argot israelí para “frenesí”), por miedo a que se revelara su identidad o sus datos. El asunto finalmente terminó en una investigación de la Autoridad de Privacidad israelí por sospecha de negligencia, cuyo resultado se desconoce.

Dos años y medio después, a principios de 2024, la aplicación Atraf volvió a cobrar vida y, casi al mismo tiempo, se aprobó la Enmienda 13 a la Ley de Protección de la Privacidad de Israel, cuyas disposiciones entrarán en vigor en agosto de 2025 y actualizan y aclaran la legislación en la materia. La enmienda establece disposiciones nuevas y avanzadas y proporciona herramientas de aplicación eficaces en línea con los desafíos de la era digital, con la intención de aumentar la protección del derecho fundamental a la privacidad y fortalecer la lucha contra las amenazas cibernéticas. Impone responsabilidad a las empresas en el ámbito de la protección de la privacidad y aumenta la supervisión de la posesión y el comercio de bases de datos, al tiempo que impone elevadas sanciones financieras en caso de infracción. También crea responsabilidad personal para directores y ejecutivos. Esto significa que si una empresa no se preocupa por proteger la privacidad de sus clientes, sus directores y ejecutivos pueden ser personalmente responsables tanto a nivel civil como penal. La enmienda también corrige una distorsión histórica de la ley, que en la práctica requería que casi cualquier pequeña empresa tuviera una licencia de base de datos (un requisito que en la práctica no se podía hacer cumplir en absoluto). Después de la enmienda, ya no es necesario registrar bases de datos pequeñas, con la excepción de las bases de datos destinadas a intercambiar información. También actualiza y aclara la cuestión de lo que se considera "datos sensibles", para los cuales existe una obligación de informar para cualquier tamaño de base de datos, todo ello cumpliendo con las normas internacionales, incluido el Reglamento de Protección de Datos de la UE (GDPR).

Aunque la ley actualmente no determina explícitamente la identidad de la entidad corporativa que supervisa la implementación de los requisitos, un documento de posición de la Autoridad de Privacidad de Israel con fecha de enero de 2024 establece obligaciones detalladas que son responsabilidad del consejo de administración y requiere que los miembros del consejo de administración no solo participen en la supervisión y el control, sino que también aprueben los procedimientos de seguridad de la información, realicen estudios de riesgos y garanticen la protección de los datos. Esto crea un estándar de cuidado y expone a los directores a una responsabilidad personal de una manera similar a lo que se decidió, por ejemplo, ya en 1996 en la Corte de Delaware, EE. UU.\*\*, donde los accionistas de la empresa Caremark presentaron una demanda derivada contra los directores con el argumento de que no habían establecido controles internos adecuados. En ese caso, la Corte Americana sostuvo que el directorio de la empresa incumplió el deber de implementar sistemas de control y monitorearlo.

A la luz de lo anterior, es extremadamente importante que cualquier empresa que mantenga una base de datos cree procedimientos adecuados y un plan de cumplimiento interno que no solo garantice la protección de los datos, sino que también proteja a los directores y ejecutivos en caso de un riesgo para la información. Es muy importante que dicho procedimiento y el plan de cumplimiento interno se elaboren en colaboración con asesores legales con un profundo conocimiento de la materia, quienes también estarán involucrados en los procedimientos para implementar el plan y hacerlo cumplir.

---

\*La abogada Osnat Nitay forma parte del equipo jurídico de Afik & Co. ([www.afiklaw.com](http://www.afiklaw.com)). La Sra. Nitay es licenciada en Derecho por la Facultad de Ciencias Sociales de la Universidad Hebrea de Jerusalén y posee un certificado de mediación familiar del Centro Gevim. Esta descripción general no constituye asesoramiento legal y se recomienda consultar a un abogado especializado en este campo antes de tomar cualquier decisión sobre los temas descritos en esta descripción general. Para más detalles: 03-6093609, o por correo electrónico: [afiklaw@afiklaw.com](mailto:afiklaw@afiklaw.com)