Israel - Cybersecurity

TABLE OF CONTENTS

August 2020

1. GOVERNING TEXTS

1.1. Legislation

Israel's cybersecurity related legislation comprises several laws and regulations covering various aspects of the cybersecurity sphere, as further detailed below.

The primary Israeli law governing data protection is the Protection of Privacy Law, 5741-1981 ('the Law'), enacted in 1981. The Law applies to any entity that manages or possesses a 'database', including both private and public entities. A 'database' is defined in the Law as a collection of personal data maintained in electronic form, excluding:

- a collection of personal data maintained for personal use rather than for business purposes; and
- a collection that includes only names, addresses, and contact information, and which by itself does not create any characterisation that invades the privacy of the persons whose information is included therein.

The Law requires certain databases to be registered with the Registrar of Databases, which operates within the Privacy Protection Authority ('PPA'), as further detailed in section 3.3. In addition, according to the Law, certain organisations are required to appoint an information security officer.

The Protection Of Privacy Regulations (Data Security) 5777-2017 ('the Data Security Regulations') is an omnibus set of rules promulgated by the Israeli Parliament ('Knesset') in March 2017, effective as of May 2018. These regulations require Israeli organisations, companies, and public agencies that own, manage, or maintain a database containing personal data, to implement prescriptive security measures, with the objective to prevent cybersecurity incidents. These include, for example, physical security measures, access control measures, cyber risk assessments, and periodic penetration test.

The Israeli Computers Law, 5755-1995 (only available in Hebrew here) ('the Computers Law'), is mostly a penal statute, specifying certain computer-related conduct comprising criminal offenses punishable by imprisonment:

- Section 2 of the Computers Law penalises any intermeddling with the ordinary operation of a computer or with its use (i.e. denial of service attacks);
- Section 4 of the Computers Law penalises unlawful intrusion into computer material (i.e. hacking and unauthorised access);

- Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony; and
- Section 6 of the Computers Law penalises the programming of computer software, or its modification, made for the purpose of unlawfully performing any one of six enumerated acts. These acts comprise, among others, interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. Section 6 of the Computers Law also deals with the act of trafficking in or installing such computer programs.

The Regulation of Security in Public Bodies Law, 5758-1998 ('the Security of Public Bodies Law'), authorises the Israeli Security Agency and the National Cyber Directorate ('NCD') to issue binding directives to organisations operating critical infrastructures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecommunications and internet providers, transportation carriers, the Tel Aviv Stock Exchange ('the Stock Exchange'), the Israeli internet Association ('the Israeli ccTLD Registry'), utility companies, and others.

The Defense Export Control Law, 5766-2007, and its regulations, govern the State's control of the export of defence equipment, the transfer of defence know-how, and the offering of defence-related services, for reasons of national security, foreign relations, international obligations, and other vital interests of the State of Israel.

In 2018, the Israeli Government ('the Government') published a proposal for a Cyber Defense and National Cyber Directorate Bill ('the Bill'). The Bill proposes to grant far-reaching and unprecedented powers to the NCD, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry out acts on the organisation's computerised material, for the purpose of handling cyberattacks.

In May 2020, amid the spread of the COVID-19 ('Coronavirus') pandemic in Israel, the Israeli government published a draft bill (only available in Hebrew here) ('the ISA Bill'), followed by a formal bill seeking to direct the Israeli National Security Agency ('INSA' and colloquially named 'Shabak' or 'Shin Bet') to engage in ubiquitous cellular-network based tracking of the whereabouts and movements of Israelis. The ISA Bill follows the Israeli Supreme Court judgment that this form of tracking of individuals (which was already carried out in Israel from March to May 2020 pursuant to provisional emergency regulations), cannot be legalised through a governmental resolution and requires a primary legislative act.

The ISA Bill would authorise INSA to process identification information, location information, and telecommunication information of Israelis (but not the content of such communications) in order to easily locate and notify them when they have been exposed to a person confirmed to have contracted coronavirus. It would also authorise the INSA to provide to the Israeli Ministry of Health ('MoH') information about individuals who were in proximity to that person during the previous 14 days. According to the ISA Bill, the INSA's authority would be subject to a governmental directive approving the tracking for renewable periods of 21 days. The authorisation may be general or specific to particular situations, and the Knesset may repeal the government's directive. The ISA Bill passed its first reading in the Knesset and may pass into law in the near future.

The ISA Bill further provides that the MoH is required to notify the person with the virus that it will be obtaining such information about them from INSA and of how the person may receive more information about the MoH's request. The MoH is bound to confidentiality and is prohibited from disclosing or transferring the data to any third party. Disclosure of a person's personal information in violation of the law would be a criminal offense punishable by up to three years imprisonment. The INSA will not use the information to corroborate compliance with quarantine requirements and the information will not be used as evidence in any investigation or legal proceeding.

Every two weeks, the INSA would be required to report the number of requests it has processed for the MoH to the Knesset's committee overseeing the issue. It will also report the aggregate number of people who near a person who contracted the virus, the status of data deletion, and any irregular eventualities that may have occurred. The MoH will also provide the parliamentary committee with similar reports, including reports assessing how effective the assistance of the INSA is (i.e. how many people exposed to Coronavirus were able to be identified only with the assistance of the INSA).

In the meantime, while the overall ISA Bill is deliberated in the course of July, the Knesset has approved an interim measure (only available in Hebrew here), valid only in the course of July, during which the INSA will be authorised to use mobile network location data to support the MoH efforts, subject to various limitations and restrictions.

1.2. Regulatory authority

The PPA within the Israeli Ministry of Justice (formerly known as the Israeli Law, Information and Technology Authority ('ILITA')), is the Israeli privacy regulator. The PPA is responsible for enforcing the Law, and has investigative powers in relation to violations of the Law and the Data Security Regulations, including on issues relating to the cybersecurity of databases containing personal data.

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Banking Supervision Department ('the Supervision Department') within the Bank of Israel. The Supervision Department is responsible, among other issues, for enforcing the data breach rules relating to cybersecurity incidents for banks and credit card companies.

The Capital Market, Insurance and Savings Authority ('the Capital Market Authority') operates within the Israeli Ministry of Finance.

The Capital Market Authority is responsible for enforcing the data breach rules relating to cybersecurity incidents at these organisations.

In 2015, the Government established a National Cybersecurity Authority ('the Cybersecurity Authority'), and in 2018 merged that same with the National Cyber headquarters who was tasked with national capabilities in cyberspace. The resulting merger is the NCD. The executive decision on the establishment of the Cybersecurity Authority prescribes its primary roles as follows:

- to manage, control, and carry out the overall, nationwide operational efforts to protect cyberspace;
- to operate a national, economy-wide Computer Emergency Response Team;
- to strengthen and reinforce the economy's resilience, through preparatory measures and regularisation;
- to design and implement a national cyber-defence doctrine; and
- to perform such duties as the Prime Minister may determine, consistent with the Cybersecurity Authority's designated mission.

1.3. Regulatory authority guidance

Over the past several years, the PPA has issued guidance to various market sectors concerning compliance with the Law. The guidelines reflect the Israeli privacy regulator's position on interpretation of the Law and clarify the PPA's position on various matters.

In particular, the following guidelines have been issued by the PPA:

- guidance on the use of CCTV and storage of CCTV footage (only available in Hebrew here);
- guidelines covering use of CCTV in workplaces (only available in Hebrew here);
- guidance on the outsourcing of data processing operations (only available in Hebrew here);

- guidance on requirements for user authentication when providing remote access to personal data (only available in Hebrew here);
- guidance on restrictions of financial institutions' use of information concerning attachment orders for sequestration issued against their clients' financial property (only available in Hebrew here);
- Guideline No. 2/2012 on Applicability of the Provisions of the Law on Screening Procedures for Admissions to Work and Sorting Institutes Activities (only available in Hebrew here);
- Clarification for Sorting Institutes Regarding the Right of Reference for Examiners for Work (only available in Hebrew here);
- guidance on the allocation of responsibility for databases between health insurers and primary health care providers (only available in Hebrew here);
- guidance on direct mailing and direct mailing services (only available in Hebrew here);
- guidance on collection of data from minors;
- draft guidance concerning privacy in the workplace (only available in Hebrew here);
- draft guidelines on the transfer and sharing of personal information in the context of mergers or acquisitions (only available in Hebrew here);
- guidance on the use of drones (only available in Hebrew here);
- guidance for municipalities on privacy aspects of smart cities (only available in Hebrew here);
- recommendations on data protection issues relating to the use of drones (only available in Hebrew here);
- clarifications on political parties' responsibility to protect personal data when using third-party applications during an election campaign (only available in Hebrew here);
- review of digital monitoring tools used around the globe amid the Coronavirus pandemic and proposed operational models for such tools (only available in Hebrew here);
- guidance on workplace privacy amid the Coronavirus pandemic (only available in Hebrew here; summary of an earlier version of this guidance, in English, is available here);
- general Q&As on privacy amid the coronavirus pandemic (only available in Hebrew here);
- guidance on schoolchildren privacy amid the Coronavirus pandemic (only available in Hebrew here); and
- background review of the data protection impact of social ranking solutions (only available in Hebrew here).

In addition, the following guidelines have been issued by the Supervision Department:

- circular on cyber-defence management at banking corporations and credit card companies (only available in Hebrew here) ('the Circular on Cyber-defence Management');
- guidelines to banks and credit card companies regarding their use of cloud computing services (only available in Hebrew here) ('the Guidelines on Cloud Computing');
- circular requiring banks and credit card companies to manage and monitor the cybersecurity risks associated with service providers who are involved in processing sensitive business or personal data (only available in Hebrew here) ('the Circular on Cybersecurity Risks');
- circular on management of operational risks (only available in Hebrew here) 'the Circular on Operational Risks');
- circular on business continuity management (only available in Hebrew here) ('the Circular on Business Continuity Management'); and
- circular on digital banking services (only available in Hebrew here) ('the Circular on Digital Banking Services').

One of the Circular on Cyber-defence Management's operative sections requires that banking corporations and credit card companies appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. The Circular on Cyber-Defence Management also specifies that banking corporations are expected to regularly identify and evaluate cyberthreats and risks and details the requirements for an effective process for doing so. Furthermore, the Circular on Cyber-defence Management points out that banking corporations ought to continuously examine the effectiveness of the various cyber-defence controls that they have established, using tools such as vulnerability reviews and controlled-intrusion tests.

The Guidelines on Cloud Computing specify how banks and credit card companies should manage the risks involved in using cloud services for data processing. The Guidelines on Cloud Computing provide, among other things, that banks and credit card companies may only use cloud services if the data is stored and processed in Israel, or through a cloud service provider that adequately protects personal data pursuant to EU data protection legislation.

The Circular on Cybersecurity Risks requires banking corporations to audit the service providers they use, impose data security obligations on the providers, and ensure that the providers comply with those obligations.

The Circular on Operational Risks requires banking corporations, (in addition to the requirements in the Guidelines on Cloud Computing), to identify, monitor, and manage technological risks by:

- implementing the same principle of managing operational risks by corporate governance and monitoring to ensure that the technology risks are aligned with the banking corporation's agenda;
- establishing policies and procedures for risk assessment; and
- auditing and monitoring procedures to mitigate technology risks.

The Circular on Business Continuity Management requires banking corporations to implement procedures for data backups and recovery and a data breach response and recovery policy, as well as procedures for remote access to the banking corporation's systems.

The Circular on Digital Banking Services requires banking corporations to perform an initial and periodic assessment of the risk for digital banking solutions used; and implement monitoring measures to mitigate the risks for customers such as monitoring of irregular activities, increasing customer awareness, and implementing proper procedures for customer identification.

Moreover, the Capital Market Authority has issued the following guidelines:

- circular on Cyber Risk Management at Institutional Entities (only available in Hebrew here) ('the Circular on Cyber Risk Management'); and
- institutional entities circular on 'Instructions for Information Security Risk Management at Institutional Entities' (only available in Hebrew here) ('the Circular on Information security Risk Management').

The Circular on Cyber Risk Management, which entered into force on April 2017, applies to all institutional investors in Israel. Its declared objective is to provide 'principles regarding the protection of an institutional entity's assets for the purpose of ensuring the rights of stakeholders and policyholders, by safeguarding the confidentiality, integrity and availability of information assets, information systems, business processes and the proper functioning of the entity.'

According to the Circular on Cyber Risk Management, cybersecurity risk management includes actions for preventing, neutralizing, investigating, and addressing cybersecurity threats and incidents to mitigate their effects and damage before, during, and after they occur. The Circular on Cyber Risk Management repealed the Circular on Information security Risk Management. The Capital Market Authority's cybersecurity requirements include, for instance, the obligation to approve, at least once a year, a corporate policy on cybersecurity risk management. Regulated entities must appoint a chief cybersecurity officer and conduct an annual assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks. The Capital Market Authority's guidelines also require financial institutions and insurance companies to run a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

2. SCOPE OF APPLICATION

2.1. Network and Information Systems

The scope of the Security of Public Bodies Law extends only to the list of organisations expressly enumerated in the statutes' schedules. These are all organisations operating various types of critical infrastructure, including telecom and internet providers, transportation carriers, the Stock Exchange, the Israeli ccTLD Registry, utility companies, and others.

The Data Security Regulations apply to any Israeli organisation, company, and public agency that owns, manages, or maintains a database containing personal data. The Data Security Regulations create four tiers of databases, each subject to an escalating degree of information security requirements and security measures. The triggering criteria for each tier relates to the number of data subjects involved, the data's sensitivity (i.e. special categories of data), and the number of people with access credentials.

The Bill has broad implications for operators of essential infrastructures, systems, or services, including internet and communications service which are considered protectable vital interests. This Bill extends to organisations operating essential infrastructures, systems or services, and which are susceptible to activities designed to impair the use of a computer or computer material.

2.2. Critical Information Infrastructure Operators

The scope of the Security of Public Bodies Law extends only to the list of organisations expressly enumerated in the statute’s Schedules 1, 2, 4, and 5.

2.3. Operator of Essential Services

The scope of the Security of Public Bodies Law extends to the list of organisations expressly enumerated in the statute’s Schedules 1,2,4, and 5. These include, inter alia, communication service providers, chemicals and oil companies, transportation service providers, the Bank of Israel, Israel Electric Corporation, and various government bodies., etc.

The Bill would grant the NCD certain authority over any organisation (including the State, local authorities, businesses, and anyone providing public service) that deals in matters of essential public interest, such as:

- state security, public security, or public safety;

- human life;
- state economy;
- essential infrastructure, systems or services, including internet and communications services;
- organisations providing services on a significant scale;
- environmental or public health;
- significant assets of personal data; and
- other interests declared by the Prime Minister.

2.4. Cloud Computing Services

There are no specific references to cloud computing services as covered entities in Israeli primary or secondary legislation.

2.5. Digital Service Providers

There are no specific references to digital service providers as covered entities in Israeli primary or secondary legislation other than the Security of Public Bodies Law which list the Israeli ccTLD Registry and communication providers that are subject to the law, since they operate critical infrastructures.

2.6. Other

Not applicable.

3. REQUIREMENTS

3.1. Security measures

The Data Security Regulations create four tiers of databases, each subject to an escalating degree of information security requirements and security measures:

- Tier One comprises databases maintained by individuals (e.g. by a sole proprietor or a corporation with a single shareholder, or a database to which no more than three people have access credentials);
- Tier Two comprises databases subject to the basic level of data security (i.e. those that do not fall within any other category, including many employee and human resources

('HR') databases);
- Tier Three comprises databases subject to intermediate data security (i.e. those to which more than ten people have access credentials or whose purpose includes making information available to other parties); and
- Tier Four comprises databases subject to the highest level of data security (i.e. those whose purpose includes making information available to other parties, or database to which either more than 100 people have access credentials or the number of data subjects therein is at least 100,000).

The Data Security Regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data. In addition, any organisation that is subject to the Data Security Regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Additionally, organisations that hold certain 'sensitive information' are required, under the Data Security Regulations, to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individuals' private affairs, including:

- individuals' behaviour in the private domain;
- health or mental condition;
- political opinions or religious beliefs;
- criminal history;
- telecommunication meta data;
- biometric data;
- financial information regarding individual's assets, debts and economic liabilities; and
- consumption habits of an individual which may be indicative of the above-mentioned types of data.

The Data Security Regulations require anyone who owns, manages or maintains a database containing personal data to implement the following information security measures:

- draft a database specification document;
- map the database's computer systems;
- maintain physical and environmental security controls;
- develop various data security protocols;
- perform annual reviews of security protocols;

- establish access credentials and manage those credentials on the extent necessary for users to perform their work;
- employ workers in database-related positions only if they have an appropriate level of clearance in relation to the database's degree of sensitivity and provide them training with respect to information security;
- maintain and document information security incidents;
- restrict usage of portable devices;
- segregate the database related systems from other computer systems;
- implement telecommunication security for computer systems connected to the internet;
- engage with data processors only after performing a proper information security due-diligence and bind them to an information security agreement; and
- keep records, documents, and decisions to demonstrate compliance with the regulations.

The Data Security Regulations introduce additional requirements applicable to databases subject to the intermediate level of security. The following requirements apply in addition to the above requirements applicable under the basic level:

- access to the database's physical premises shall be monitored;
- equipment brought in or taken out of the database's physical premises shall also be monitored;
- an extended data security protocol shall cover, among other issues, user authentication measures applicable to the database, backup procedures, access controls and periodic audits;
- users with access privileges shall be authenticated with physical devices such as smart cards;
- a protocol shall be established for means of identification, frequency of password change and response to errors in access control;
- an automated mechanism for monitoring access to the database shall be established;
- audit logs shall be maintained for at least two years;
- either an internal or external audit shall be performed at least once in 24 months; and
- a backup and recovery plan shall be established.

The Data Security Regulations introduce additional requirements applicable to databases subject to the highest level of security. The following requirements apply in addition to the requirements applicable to those under the basic and intermediate level:

- the database owner shall perform a risk assessment once every 18 months, using a qualified professional;
- the database's computer systems shall be subjected to penetration tests once in 18 months; and
- security incidents shall be reviewed at least once every calendar quarter, and an assessment shall be made of the need to update security protocols.

3.2. Notification of cybersecurity incidents

There are several provisions of Israeli law according to which certain organisations are required to report cybersecurity incidents.

Effective since May 2018, the Data Security Regulations establish a data breach notification requirement in Israel. Under the Data Security Regulations, owners of databases designated within an 'intermediate' or 'high' tier of security are required to notify data breaches to the PPA. The notification obligation for database at the intermediate level of security applies when the breach extends to any material portion of the database, while the notification obligation for database at the high level of security applies to any breach, regardless of its scope or materiality.

The notification must state the measures taken to mitigate the incident. In effect, the notification obligation depends on the database's security level, which in turn depends on the nature of the information stored in the database.

The intermediate level of security applies to public agencies, organisations that hold sensitive information and data brokers. The high level of security applies to organisations that hold sensitive information and to data brokers, where the database extends to at least 100,000 data subjects or if more than 100 persons have access credentials to the database.

In certain circumstances, the PPA may order the organisation, after consultation with the Head of the National Cybersecurity Authority (now replaced by the NCD), to report the incident to all affected data subjects. Generally, if the breached data is not capable of identifying an individual, then the incident does not need to be reported, since it does not pertain to regulated 'personal data.'

In July 2019, following the first anniversary of the Data Security Regulations, the PPA published a report (only available in Hebrew here) ('the Report') summarising its enforcement activities relating to data breaches. According to the Report, the PPA carried out 146 instances of administrative en-

forcement action against organisations in relation to data breaches classified as 'severe.' However, the PPA was only notified about 103 of those breaches. The remaining 43 breaches were investigated after the regulator either received complaints about them, or proactively discovered them.

Banks and insurance companies are required to report any cybersecurity incidents and data breaches pursuant to regulatory guidelines by the Supervision Department. Insurance companies and financial institutions are required to report any cybersecurity incidents and data breaches to the Capital Market Authority.

The INSA also published a position paper emphasising a public company's duties of disclosure both of general cybersecurity risks that a company faces as well as of specific incidents having material adverse effects on the company (only available in Hebrew here).

3.3. Registration with a regulatory authority

The Law requires that certain databases be registered with the Registrar of Databases, which operates within the PPA. The Law's provisions governing database registration apply to owners of databases that meet any of the following criteria:

- contain data about more than 10,000 persons;
- contain sensitive data;
- contain data about persons where the data was not provided by such persons, was not provided on their behalf, or was not provided with their consent;
- belongs to certain government bodies; and
- is used for direct marketing.

However, the Registrar of Databases may require registration of a database that is otherwise exempt from registration, though this decision is appealable. The database registration system is database-driven and not owner-driven. Hence, if a database owner has several databases, it must register each database separately.

The Law sets forth the basic format of a database registration, requiring that an application to register a database include the following information:

- the identities and addresses of the owner and, if applicable, the holder (i.e. processor) of the data;
- the purposes of the database;
- the types of data contained in the database; and

- the information concerning data transfers abroad and the receipt of data from public bodies.

3.4. Appointment of a 'security' officer

Under the Law, certain organisations are required to appoint an information security officer responsible for information security of in their databases. These organisations include public entities, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance and creditworthiness evaluation.

The Security of Public Bodies Law, requires certain public organisation listed under Schedules 4 and 5 of the statute to appoint a person responsible for securing essential computer systems in those organisations.

3.5. Other requirements

To ensure the data security officer's independence, the Data Security Regulations require that the officer must be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. The Data Security Regulations prohibit the officer from being in a position that raises a conflict of interests. Substantively, the Data Security Regulations require the officer to establish data security protocols and an ongoing plan to review compliance with the Data Security Regulations. The officer must present findings of its review to the database manager and to the officer’s supervisor.

4. SECTOR-SPECIFIC REQUIREMENTS

Cybersecurity in the health sector

In 2015, the General Manager of the Israeli MoH issued a data security circular alerting all medical institutions (clinics, health maintenance organisations and hospitals) to the importance of cybersecurity and requiring them to certify to ISO 27799 on data security in healthcare related information systems. Certification to this standard is a pre-requisite to obtaining or renewing the medical institution's permit. According to this circular, medical institutions may only use service providers who themselves are certified to either ISO 27001 or ISO 27799.

The Israeli MoH also established a policy for cybersecurity in medical devices, which establishes the cybersecurity requirements for medical devices used in Israel. The guidelines are directed both to manufacturers and importers seeking to market medical devices in Israel, and to health care providers using medical devices in the treatment of patients. The guidelines describe a myriad of essential and non-essential cybersecurity controls. Essential controls include access restriction, disaster recovery and resilience, and encryption of wireless transmission. The guidelines also prescribe the cyber risk-management measures that health care providers must implement when purchasing, installing, and using medical devices.

Cybersecurity in the financial sector

The Supervision Department at the Bank of Israel is responsible, among other issues, for enforcing the data breach rules relating to cybersecurity incidents at banks and credit card companies. The Supervision Department has issued various regulatory requirements and guidelines for banks and other financial institutions regarding privacy and cyber security such as the ones detailed in section 1.3 above.

In addition, the PPA published specific guidelines on financial institutions' compliance with the Data Security Regulations. These guidelines indicate which provisions of the Data Security Regulations apply to specific categories of covered entities in the financial sector:

- Guidelines on compliance with the Data Security Regulations for Stock Exchange members who are not banks but are subject to the Stock Exchange Market protocol (only available in Hebrew here);
- Guidelines on compliance with the Data Security Regulations for pension fund management companies and insurance companies subject to the Capital Market Authority (only available in Hebrew here); and
- Guideline on compliance with the Data Security Regulations for financial bodies supervised by the Supervision Department (only available in Hebrew here).

Cybersecurity practices for employees

The PPA's 2017 Guidelines on the use of surveillance camera in the workplace (only available in Hebrew here) ('the PPA's Guidelines') underscore that employers may use surveillance cameras solely for legitimate purposes relevant to the workplace, and only to the extent required for such purposes. According to the PPA's Guidelines, the use of surveillance cameras in the workplace is subject to a duty of reasonableness, proportionality, good faith and fairness incumbent on the employer. Excessive use of surveillance cameras in the workplace, which is not proportionate, may put the em-

ployer at risk of administrative penalties and for criminal and civil liability. The PPA's Guidelines require employers using surveillance cameras to take measures such as conducting a privacy impact assessment, developing and establishing a privacy policy regarding the manner and scope of using cameras and the purpose of placing them in the workplace, and limiting the use of cameras for specific, legitimate purposes. The PPA's Guidelines must be published so that employees are notified. The PPA's Guidelines also state that employer should not place cameras in areas in which employees have a reasonable expectation of privacy, such as at restrooms, dressing rooms, private or shared workplace areas (provided such areas are not accessible to the public).

Israeli legislation does not specifically address the issue of employer monitoring and accessing employees' communications and files for cybersecurity purposes. The Labor Appeal no. 90/08 of *Tali Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law* (8 February 2011) of the Israeli National Labor Court expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of prerequisites and conditions for permissible access: such access must be for a legitimate purpose, proportional, and subject to the prior consent of the employees to a workplace privacy policy that transparently discloses the employer's envisioned activities of monitoring employees.

Additionally, in light of the spread of the Coronavirus pandemic the PPA has published a number of guidelines on the protection of privacy in workplaces:

- Guidelines for employers on protection of company data when working remotely (only available in Hebrew here);
- Guidelines for the protection of employees' privacy in workplaces in light of the Coronavirus pandemic (only available in Hebrew here); and
- Guidelines on privacy when entering workplaces and trade-commerce businesses in light of the Coronavirus (only available in Hebrew here).

Cybersecurity in the education sector

Not applicable.

5. PENALTIES

The PPA is authorised to inspect and search database owners for the purpose of enforcement of the Law. It is also authorised to refuse to register a database if it has reason to believe the database is intended to be used for an illegal purpose. The PPA also has the authority to seek a court order to suspend a database's registration.

A breach of the Law constitutes a strict liability criminal offense, punishable by one year of imprisonment, and also constitutes a civil tort. For example, under Section 31A(a)(6) of the Law, failure to appoint an information security officer where such is mandated by the Law is a strict lability offence punishable by up to one year in prison. The PPA is also authorized to impose administrative fines instead of criminal prosecution.

There are currently no penalties imposable by the PPA for failing to comply with the data breach notification requirement in the Data Security Regulations. A proposed amendment to the Law is aimed to empower the PPA with authority to impose penalties.

The Computers Law specifies the maximum penalties for violation of the criminal offences governed by it. For example:

- intermeddling with the ordinary operation of a computer or interference with its use carries a maximum sentence of three years' imprisonment (Section 2 of the Computers Law);
- unlawful intrusion into computer material carries a maximum sentence of three years' imprisonment (Section 4 of the Computers Law);
- intrusion into computer material committed in furtherance of another predicate felony carries a maximum sentence of five years' imprisonment (Section 5 of the Computers Law); and
- programming or modifying a computer program for the purpose of unlawfully performing any of the acts enumerated in Section 6 of the Computers Law, is punishable by up to three years of imprisonment, whereas the act of trafficking in or installing such computer programs is punishable by up to five years' imprisonment.

In relation to civil proceedings, the most prominent civil action that may be brought against a legal entity in relation to a cybersecurity incident is a class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006 (only avaliable in Hebrew here). In order for a court to certify a class action suit, the representative plaintiff must prove that:

- the action raises substantive questions of fact or law common to all members of the putative class that were affected by the incident, and that it is reasonably possible that

such questions will be resolved in the class's favour;
- under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute;
- there are reasonable grounds to assume that the interests of all members of the class will be adequately represented and conducted; and
- there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages in relation to a cybersecurity incident may assert an individual civil action based on several applicable laws, for example, invasion of privacy under the Law or negligence in accordance with the Israeli Torts Ordinance.

6. OTHER AREAS OF INTEREST

Since the data breach notification requirement took effect in May 2018, most data security incidents are detected and reported by information security researchers and 'white hat hackers.'

Even under the new data breach notification regime, the negligible number of reported breaches suggest that many go unnotified. According to the PPA's annual report, it carried out 146 instances of administrative enforcement action against organisations in relation to data breaches classified as 'severe.' However, the PPA was only notified of 103 of these breaches. The remaining 43 breaches were investigated after the regulator either received complaints about them, or proactively discovered them.

There have been very few reports of meaningful black-hat hacker (or state sponsored) data breach incidents against commercial companies. However, one of them was recently reported in the news.

ABOUT THE AUTHORS

Haim Ravia

Pearl Cohen Zedek Latzer Baratz

Haim Ravia is a senior partner and chair of the Internet, Cyber & Copyright Group at Pearl Cohen Zedek Latzer Baratz. Haim deals extensively with data protection, privacy, cyber and Internet law, IT contracts, copyright, electronic signatures and open source software. He was a member of the Israeli public commission for the protection of privacy and part of a governmental team that re-examined Israeli law pertaining to databases of personal information. Haim received an acknowledgment award from the Israel Chamber of Information System Analysis for pioneering and innovation in the Israeli Internet. Practicing Internet and Cyber law for over 20 years, he has also written numerous articles in theses subjects and operates Israel's first legal website at www.law.co.il. Haim advises to various organizations, from early-stage startups to Fortune 500 companies, including Israel's leading financial institutes and technology companies, in his area of expertise.

hravia@pearlcohen.com

RELATED CONTENT

NEWS POST

UK: ICO's Age Appropriate Design Code to come into effect 2 September 2020

NEWS POST

Estonia: DPI opens investigation into Imperal Varad OÜ regarding leak of 27,000 customers' information

LEGAL RESEARCH

NIST Special Publication 800-207 Zero Trust Architecture (11 August 2020)

NEWS POST

USA: NIST publishes special publication on cybersecurity and zero trust architecture for enterprise security infrastructure

NEWS POST

USA: BHN notifies OCR of health data breach following virus affecting their internal systems