Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

TMT

Israel
Law and Practice
Michael (Micky) Barnea, Daniel Lorber, Anat Even-Chen and Nir Abraham
Barnea Jaffa Lande & Co

chambers.com

2020

ISRAEL

Law and Practice

Contributed by:
Michael (Micky) Barnea, Daniel Lorber, Anat Even-Chen and Nir Abraham
Barnea Jaffa Lande & Co see p.13

Contents

1. Cloud Computing p.2

2. Blockchain p.5

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence p.6

4. Legal Considerations for Internet of Things Projects p.6

5. Challenges with IT Service Agreements p.7

6. Key Data Protection Principles p.7

7. Monitoring and Limiting of Employee Use of Computer Resources p.8

8. Scope of Telecommunications Regime p.9

9. Audio-Visual Services and Video Channels p.9

10. Encryption Requirements p.10

1. Cloud Computing

Cloud services provide strong benefits for companies and for individuals. These cloud-computing technologies allow efficient and convenient utilisation of computing resources, together with the ability to share resources as needed. These uses reduce the costs for the purchase of equipment, dedicated rooms for data centres, electricity, etc. The savings also lead to environmentally friendlier computing (ie, green computing).

Despite the benefits of using cloud technologies, such use can expose companies and end-users to significant risks, mostly related to privacy and data security issues.

Although Israel is known for its fast adoption of technology, the same cannot necessarily be said of Israeli laws or regulations specifically related to cloud computing.

Israel has a comprehensive protection of privacy regime, with privacy being recognised as a constitutional right under the Basic Law: Human Dignity and Liberty (1992) (Basic Law). Specific provisions dealing with infringement of the right to privacy and the use of computerised databases are included in the Protection of Privacy Law 1981 (Privacy Protection Law) and the regulations promulgated thereunder. The Israeli Privacy Protection Authority (PPA), established by thePrivacy Protection Law, regularly publishes guidelines and position papers to instruct the market on the regulator's position in light of technological developments. While legislation has not always been updated to accommodate the various developments, the PPA aims to close these gaps by way of interpretation.

The use of cloud computing creates a twofold challenge. The first is data security and the second is cross-border transfers.

Using third-party cloud-based services is considered "outsourcing". Accordingly, it must comply with the provisions dealing with such in the Privacy Protection Law and the regulations promulgated thereunder.

The most recent general legal requirements for outsourcing are set out in Regulation 15 of the Data Protection of Privacy Regulations (Data Security) 2017, which came into force in May 2018 (Data Security Regulations). Regulation 15 of the Data Security Regulations supplements the Outsourcing Guidelines published by the PPA in 2011 (Outsourcing Guidelines). Regulation 15 and the Outsourcing Guidelines instruct database owners on the contractual safeguards that must be put in place when an external service provider, defined as a database holder, is granted access to a database.

First, the database owner must assess, prior to entering an agreement with the external service provider, the data security risks involved in the engagement. This is a very important step, as these risks must already be known in order to address them in the data processing agreement and in order for the required safeguards to be put in place.

The Data Security Regulations require that data processing agreements address the following issues:

- the permitted processing activities, the purposes of such processing, and the nature of the data shared;
- the database systems that the external service provider may access;
- the duration of the processing, the manner of returning the data to the database owner at the end of the engagement or its destruction, and the relevant reporting to the database owner;
- the manner in which data security obligations are implemented by the database holder and additional data security instructions set by the database owner, if any;
- the confidentiality undertaking required of the database holder and its authorised users to protect the information confidentiality and ensure compliance with the data processing agreement;
- obligations with respect to sub-processors if the use of such is permitted;
- reporting obligations of the database holder, which will include at least annual reporting as to the manner in which the security obligations are implemented; and
- obligations in case of a security incident.

Furthermore, the Outsourcing Guidelines, while preceding the Data Security Regulations, were not terminated and remain valid. They include a list of recommendations for engagement with IT service providers, including the following.

- Refraining from delivering to the IT service provider a copy of the database. Instead, gaining access to the databases that remain under the control of the organisation.
- In the event the IT service provider collects the data directly from the data subjects, then the recommendation is to include a provision in the agreement requiring the IT service provider to comply with all applicable privacy laws (retention of data, notification, modification rights, etc).
- The organisation and the IT service provider shall both consider nominating a data security officer.
- In order to monitor compliance with the applicable Privacy Protection Law and Data Security Regulations, the organisation should perform audits at the IT service provider's premises to ensure compliance.

Complying with these requirements is a challenge for businesses when engaging with third parties, as well as for third parties providing IT services, as they must accommodate requirements from multiple database owners.

The second major legal aspect in regard to cloud computing is that it may require the transfer of personal information abroad (ie, to be stored in a jurisdiction other than the State of Israel). This legal concern is addressed in the Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001 (Transferring Information Abroad Regulations). In accordance thereto, prior to any transfer of data from an Israeli database to another database located abroad, the transferor must ensure that the level of data protection legislation in the destination country is at least as protective as the level of the Israeli legislation. For examination of the data protection level, the following principles should be taken into account:

- the data shall be gathered and processed in a legal and fair manner;
- the data shall be held, used, and delivered only for the purpose for which it was received;
- the gathered data shall be accurate and up to date;
- the data subjects have the right to inspect and correct the data related to them; and
- proper security acts shall be performed in order to protect the data in the database.

The legislator acknowledged that the abovementioned conditions might be burdensome. Therefore, even if the abovementioned principles are not met, the data can be transferred abroad in the event one of the following is applicable:

- the data subject has provided his consent to the transfer;
- if the consent of the data subject can't be obtained by the transferor at the time of the transfer, and the transfer of the information is necessary in order to protect the health or well-being of such data subject;
- the data is transferred to an entity under the control of the same database owner, and the transferor has ensured that following the transfer the privacy protection will remain unharmed;
- the data has been transferred to a person who is bound by an agreement with the database's owner, which includes provisions regarding compliance with Israeli law for the information kept in databases, mutatis mutandis;
- the data was publicised to the public, or became available for the public, in accordance with a legal authority;
- the transfer of the data is essential for public safety or security;
- the transfer of the data is required according to Israeli law; or
- the data is being transferred to a country that:
  (a) is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data;
  (b) received data from the member states of the European Community, with the same degree of acceptance; or
  (c) the Israeli Registrar of Databases (Registrar) has informed in the Israeli Official Government Gazette that there is an authority in such country responsible for the protection of privacy and that the Registrar has established an arrangement for co-operation with such authority.

One of the biggest challenges under this regulation is the limitation on onward transfers and the use of sub-processors.

It should also be noted that there are no "standard contractual clauses" as prescribed by the GDPR for Israeli companies when dealing with transfers subject to Israeli law, and the EU clauses cannot be relied on. Thus, international companies are required to make certain adaptations to their clauses when dealing with transfers outside of Israel to comply with the specific Israeli regulation applicable to data processing.

In this framework, it should also be noted that according to a European Commission decision dated 31 January 2011, Israel meets the European Union's adequate protection standards for automated processing of personal data. Therefore, information from European residents can be transferred to Israel, without approval but subject to the GDPR regulations.

Israeli law includes industry-specific regulations with respect to the use of cloud-based services, as follows.

Banking

On 13 November 2018, the Supervisor of Banks published a guideline entitled Cloud Computing (Guideline). The Guideline sets forth provisions applicable to banks and to acquirers (both referred as "banking corporations") for using cloud services. In accordance with the Guideline, banking corporations are prohibited from (i) using cloud computing for central operations or systems; and (ii) storing, transferring, or processing sensitive information in cloud computing outside the borders of Israel, unless they confirm that the cloud service provider fulfils the level of data protection required by the European Union.

The Guideline states that a banking corporation must comply with Israeli privacy protection legislation, and also determines that as for corporate governance, prior to the use of any cloud computing, such use shall be approved in advance by the board of directors of the banking corporation.

In addition to the foregoing, prior to any engagement with a service provider of cloud computing, a banking corporation shall estimate the financial outcome of the project and consider the service provider's professional record for undertaking cloud-computing services. The banking corporation shall have the right to perform periodic inspections and monitor cyber-events.

The banking corporation shall safeguard the cloud computing access channels and ensure that cybersecurity and data protection actions are performed that limit, as much as possible, the use of these channels as a way to hack the banking corporation. Similarly, the banking corporation's data should be encrypted at the time it is transferred and when it is stored in systems that are multi-tenancy. The Supervisor of Banks acknowledges that such encryption requirements may be burdensome, and therefore the Guideline states that the banking corporation must at least encrypt sensitive data that, if revealed, could harm the banking corporation or its clients.

The Guideline also refers to agreements with service providers of cloud computing, and states that such agreement shall include the following provisions.

- The banking corporation's unilateral right to terminate the engagement with the service provider and the use of its services, and the banking corporation's right to transfer the data to a different service provider, while the current service provider shall transfer the data of the database owner from its system within a short time period, shall erase such data from its system, and shall be obligated to not retrieve the data from its system.
- The information right of the banking corporation with regard to examinations and inspections performed to the cloud service provider.
- The banking corporation itself and the Supervisor of Banks should be allowed to perform inspections of the cloud computing service provider, on a risk evaluation basis.
- In the event of any change in ownership of the cloud computing service provider, the banking corporation should re-examine the engagement in order to ensure compliance with the undertakings specified in the agreement by the new cloud service provider.

Institutional Entities

On 31 August 2016, the Supervisor of the Capital Market, Insurance and Saving Authority in the Israeli Ministry of Finance published guidelines for institutional entities in Israel entitled Managing Cyber Threats in Institutional Entities (Institutional Entities Guidelines). These guidelines address the use of cloud computing in institutional entities.

The term "institutional entities" includes insurance companies, pension funds, and provident funds. The Institutional Entities Guidelines state that the following considerations should be taken into account when such institutional entities are considering using cloud computing.

- Prior to using the cloud computing system, the institutional entity should perform an evaluation of specific risks and should discuss the potential risks in a steering committee.
- Sensitive information or a client's personal information should not be stored outside the borders of the State of Israel unless the institutional entity ensures compliance with the Transferring Information Abroad Regulations and the GDPR.
- Sensitive data in cloud computing databases outside the borders of the State of Israel must be encrypted.
- Access to the data in the cloud database should be performed through an authorised address only.
- When the data of an institutional entity is stored in a multi-tenant system, technology such as encryption, data shielding, or tokenisation should be used to prevent exposure of sensitive information or a client's personal information to unauthorised bodies.
- The written agreement between the institutional entity and the cloud service provider must contain provisions regarding the right of the institutional entity to control and supervise the services rendered by the cloud computing service provider. In addition, such agreement shall include a provision regarding the institutional entity's unilateral right to terminate the engagement with the service provider. In such case, the cloud service provider shall erase the data from its system and is obligated not to retrieve the data from its system.

The CDU

The Governmental Cyber Defense Unit (CDU) published on 14 November 2019, a circular entitled Vendors' Management in the Supply Chain of Government Offices (Cyber Circular). The purpose of the Cyber Circular is to instruct government offices about the efficient management of a data security system, the minimisation of cyber-threats originating in the supply chain, and the strengthening of an office's ability to face cyberattacks.

The CDU is aimed at developing a clear methodology between the various ministries in order to face cyber-threats.

In the field of cloud services, the vendors shall comply with the provisions of the National Cyber Security Authority's (CERT) Guideline 5.5 entitled Data Security for Transition to a Public Cloud.

Compliance with these requirements will be mandatory by the end of 2020 for all governmental offices using outsourcing, including cloud computing services.

2. Blockchain

In the modern world, technology develops at a much faster pace than legislation.

Israeli law addresses virtual currency in the context of anti-money laundering and requires companies providing virtual currency wallets or exchange services to obtain a financial services licence, as further elaborated below. Legislation and regulators have yet to provide practical guidance with respect to many of the virtual currency challenges, or an holistic approach to virtual currencies, including protection of the assets ("wallets") from thefts or fraud, protection from money laundering, including transfers for the benefit of criminal and terror organisations, and other tax-related matters.

The use of blockchain-based solutions in other (non-virtual currency) areas creates material challenges in terms of cybersecurity and the protection of privacy.

When dealing with virtual currency, one of the main risks and challenges a business is faced with is how to ensure the receipt of proceeds associated with virtual currencies in Israeli banks. Because a blockchain-based solution is designed to be anonymous, it creates a risk to all parties of being involved in a money laundering operation if the source of the funds cannot be confirmed, even if the parties involved are not financial institutions and are not subject to monitoring and reporting obligations.

In order to protect the integrity of the solution and enjoy the technological benefits of blockchain, non-anonymised blockchain solutions are used. For instance, when a user makes a transaction, his or her unique code (public key) is recorded on the system. This creates a new set of data that may involve personal or personally identifiable information that is stored in multiple locations. Each user holds a unique public key and therefore it can be identified. Since the blockchain system maintains records of the transactions, this may lead to additional obligations under the Privacy Protection Law. For instance, each party on the blockchain system is subject to the obligations of database holders described in **1. Cloud Computing**, above, and the manager of the system must enter into data processing agreements with all parties and monitor their activity. In addition, one of the characteristics of blockchain solutions is that the blocks cannot be changed and the history of the transaction is always maintained. This may seem to be in conflict with a data subject's right to request deletion of the information. We note that the "right to be forgotten" is not as extensive under the Privacy Protection Law as it is under the GDPR. However, data subjects are entitled to review and correct and sometimes request the deletion of information.

With regard to the taxation of blockchain transfers, the main issue is whether to classify virtual currencies as "assets" or "currencies". In order to regulate this question, the Israel Tax Authority (ITA) published the circular Taxation of Activity Involving a Decentralized Payment Method (Known as 'Virtual Currencies') (05/2018) (the Circular). In the Circular, blockchain currencies are identified as assets, as defined under the Income Tax Ordinance [New Version] 5721-1961 (Ordinance). The Circular states that because virtual currencies are identified as assets, in accordance with the Ordinance, the sale of a virtual currency shall be deemed the sale of an asset, and the income shall be regarded as a capital gain, which is taxed in accordance with the Ordinance.

The Circular also states that with regard to mining activity, any income arising therefrom shall be regarded as business income, and therefore is taxed as such.

On 19 May 2019, Judge Shmuel Bornstein of the Central District Court (in the Koppel case) ruled that virtual currencies should be classified as assets and not as currencies. Thus, the district court adopted the ITA position on the matter.

With respect to the public offering of virtual currencies, on 5 March 2019, the Israel Securities Authority published the final report of the Committee to Examine the Regulation of a Decentralized Cryptographic Currency Issuance to the Public (Committee).

The Committee examined initial coin offerings (ICOs) and stated that, as of March 2018, the number of ICOs had radically decreased, with most of the participants being sophisticated investors. The ICOs referred to the crypto-assets as "securities" and therefore the public offering was in accordance with the applicable regulation. The Committee urged the Israel Securities Authority to provide dedicated tools to contribute to and support technological development while maintaining the interests and protection of investors. The Committee suggested establishing (i) a dedicated disclosing method, (ii) a regulatory sandbox to provide a dedicated regulatory environment for companies using the technology, and (iii) a dedicated platform for trading crypto-assets.

In addition, offering wallet services is regulated as a "service in a financial asset" and requires companies offering such services to hold a valid financial services provider licence pursuant to the Supervision of Financial Services Law (Regulated Financial Ser-

vices) 2016. Licence holders are subject to anti-money laundering requirements. Companies active in this field are waiting for the promulgation of relevant anti-money laundering regulation, which will provide guidance and instruction on the obligations of licence holders in this respect.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

Big data analytics help organisations harness their data and use it to identify new opportunities. This, in turn, leads to smarter moves, more efficient operations, higher profits, and happier customers.

The benefit of using technology is huge, but the technology may be risky and infringe on human rights. While there are no specific laws and regulations in Israel addressing big data, machine learning and artificial intelligence, there are specific fields in which exists a reference to the adoption of big data technologies.

The National Digital Program of the Israeli government was formulated based on the primary goals and the strategic objectives of the National Initiative, as defined in Government Resolution No 1046 (Plan).

The Plan states that digitalisation processes – mainly in the fields of health, education, social services, economy, and housing, including big data technology and informed use of the enormous amounts of data that are available – will be available in the future for the public sector. This offers a unique opportunity for a quantum leap in how government work is managed and in its decision-making processes.

With regard to the health and medical field, per a statement by the Israeli government published on 25 March 2018, following and in accordance with the Digital Israel program, the government has approved a five-year national digital health programme designed to personalise medicine, improve medical procedures, and keep Israel at the forefront of the medical-tech field. The Israeli government will regulate the digitisation and sharing of data and will promote and finance collaboration with commercial companies focused on big data technologies.

The governmental initiative is beneficial, but it raises concerns about the safeguards to be implemented when transferring a huge body of personal data to the business community.

In the framework of health and medical big data, two Israeli Minister of Health circulars (MOH Circulars) detail the benefits and advantages of the adoption of big data technologies by the health system in Israel. They are both dated 17 January 2018, and are entitled Collaborations Based on Secondary Uses of Health Information and Secondary Uses of Health Information. The MOH Circulars encourage collaboration between Israeli health organisations and companies engaged in the development of medical technologies, while also protecting the sensitive personal information of the patients, in accordance with the following: the Privacy Protection Law, 1981; the Patient Rights Law, 1996; the Privacy Protection Regulations (Terms of Information Retention and Retention and Information Transmission Regulations between Public Bodies), 1986; the Privacy Protection Regulations (Security of Information), 2017; the Privacy Protection Order (Determination of Public Bodies), 1986; and the Transferring Information Abroad Regulations, as set forth in **1. Cloud Computing**.

Meanwhile, the use of machine learning and artificial intelligence has created concerns that automated decisions will be discriminatory to certain persons or groups in the population. While Israeli law has yet to specifically address such circumstances, various legal provisions provide recourse to people who are discriminated against. Therefore, companies implementing artificial intelligence or machine-learning solutions should be aware of the grievances that may arise out of the discriminatory or offensive outcomes of an automated decision-making mechanism and mitigate such potential results.

4. Legal Considerations for Internet of Things Projects

The Internet of Things (IOT) is considered the second internet revolution. Many devices will become "smart" devices, connected to the internet. While the benefits are well known, the risks inherent in this technology are also high. These risks mainly involve cyber-threats, big data regulation, and the protection of users' privacy.

The PPA has published a few guidelines indicating its growing interest in IoT, such as the guideline on privacy in smart cities (December 2018) and the guideline on the use of drones (23 December 2018).

There are no specific laws or regulation addressing this subject matter, but, in a guideline dated 25 November 2018, the PPA urges companies and manufacturers to adopt the privacy-by-design method (ie, to embrace privacy considerations) in each project and in all the aspects of the products or systems. This includes:

- developing a new computing system for storing personal information or accessing personal information;

- promoting internal policies or strategies that may have privacy implications;
- creating initiatives for exporting and sharing personal information; and
- using the collected personal information for new purposes.

Although this method is not mandatory under Israeli law, the PPA believes that using it can be beneficial for the protection of privacy, and will provide companies with a better early understanding of problematic issues that may arise from new developments.

As one of the PPA's roles is to educate the public and raise privacy awareness, the PPA has just recently translated the information prepared by the National Data Protection Commission (CNIL) regarding various smart devices and included privacy enhancing recommendations for users. This is a common regulatory technique utilised by the PPA in the absence of any specific regulation or infringement event. This publication emphasised that the PPA considers voice to be a personal identifier and signalled that any data breach involving such devices will be an issue for those entities who offer them in Israel.

5. Challenges with IT Service Agreements

The response to **1. Cloud Computing** provided a detailed description of the legal framework for outsourcing IT services.

Israeli and foreign companies frequently examine the appendices addressing data security and the transfer of information in various agreements. Hence, appropriate solutions should be provided at both the legal and technological levels. At the legal level, the appendices may address and include references to commercial terms of indemnity, liability, and risk allocation between the parties.

The Data Security Regulation require that data security means implemented are "reasonable" and "adequate". These are vague standards and one of the biggest challenges for every business, and especially for small and medium-sized businesses, using IT services is to determine reasonableness on a budget.

6. Key Data Protection Principles

The right to privacy in Israel gained a constitutional status with the adoption of the Basic Law. Section 7(a) of the Basic Law provides that every person is entitled to privacy.

The Privacy Protection Law, and the regulations promulgated thereunder, is Israel's principal data protection legislation. It applies, inter alia, to the protection of all personal information, and sets forth the obligations of individuals and entities on how they must hold and manage such information. The Privacy Protection Law does not protect the privacy of corporations but only the privacy of individuals. One of the areas regulated by the Privacy Protection Law is the requirement of holders of certain types of "information" to register a database and maintain it in a certain manner provided for thereunder. The Privacy Protection Law defines "sensitive data" as "data regarding a person's personality, privacy, health, financial situation, ideas and beliefs, and data that was ordered to be regarded as sensitive data by an order of the Minister of Justice".

In addition to the general right to privacy, Amendment 4 (Databases) defines "database" in Section 7 of the Privacy Protection Law as follows: "a collection of information that is held by magnetic or optical means and that is intended to be processed by a computer", excluding:

- collection for personal use (ie, not for business purposes); and
- collection that includes only names, addresses, and connection possibilities, which, by itself, does not create a characterisation that may violate the privacy of the individuals whose names are mentioned, and under the condition that the owner of the collection does not control any additional collection.

As mentioned above, the Privacy Protection Law requires certain databases to be registered with the Registrar. This applies to databases containing sensitive personal information or personal information about more than 10,000 data subjects (ie, most databases). While the registration obligation is on the database owner, database holders are prohibited from providing services to databases that are not duly registered.

The Data Security Regulations effective as of May 2018 clarify the internal controls required from a database holder and set out the expected data security steps to be taken by the database holder, emphasising broader substantive responsibility of holding and processing personal data.

The Data Security Regulations require the database owner to prepare a database specification document. This document must include a description of the purpose of the database, the types of data contained in the database, if there is a cross-border transfer of data from the database, the main data protection risks, and the measures to mitigate such risks. The database owner is required to examine, at least once a year, the need to update the database specification document, and to further examine

whether the database contains more data than is necessary for the purpose of the database.

The Data Security Regulations require the database holder to adopt proper security measures considering the sensitivity of the data and the risks identified. The holder must also provide a list of specific data security issues to be addressed, such as creating a back-up of the database, analysing documented security events at least once a year, and broadening the definition of "authorized person" (ie, a person with authorised access to the database) to include persons with authorised access to (i) the data, (ii) the database systems, or (iii) any information or component required to activate or access the database.

Finally, the Data Security Regulations impose on entities who suffered a material security event the obligation to report to the PPA within 72 hours of the event.

7. Monitoring and Limiting of Employee Use of Computer Resources

For decades, employers have had an interest in monitoring employees. As far back as 200 years ago, the English philosopher Jeremy Bentham proposed an architectural structure in which the manager sat on an elevated floor in the centre of the factory to allow full control, surveillance, and supervision of his workers. In the age of modern technology, where almost every employee is equipped with a computer, an email box, a mobile phone (also used as a computer), and detection and GPS devices that enable accurate employee information retrieval, employers can easily track their employees.

Today, a special physical structure is no longer required to keep track of employees. Any employer can, without incurring special expenses, "view" the employee's emails and acquire personal information, look at websites the employee is browsing, observe who the employee usually talks to over the phone, and track the places the employee visits during the day. This accessible information contains, in many cases, personal and private information, such as employee medical information, family information, or other personal matters, of which the employer has no need to be aware.

The main requirements of an employer are similar to the general rules of privacy in Israel – pursuing a legitimate purpose with proportionality, restriction of the purpose, a good faith mandate that the collection of information of an employee is done solely for legitimate purposes relating to employment relations, and determining if the employer's monitoring is not too excessive and if there are less intrusive measures that could have been taken instead.

The issues of employee monitoring and limiting use by employees of a company's computer resources were specifically addressed in a general collective bargaining agreement registered in 2008 (CBA). The CBA governs the obligations and rights of employees and employers with respect to computer use and the rules of conduct in the workplace, wherein the employee uses the employer's computer. The CBA balances the rights of the employer with those of the employee. According to the CBA, generally, the employee shall use the computer for work use and may, in accordance with the general rules of the CBA and the law, use the computer for personal use as well, but with proportionality and only for a reasonable duration of time.

In 2011, the Israeli National Labor Court set a major precedent (in the Isakov case). The court differentiated between an email account provided to the employee as part of his employment and a personal email account. The court held that in a work email account the employer has limited monitoring rights subject to the principles of transparency and proportionality. If an email account also contains personal contents, the employer may monitor it in exceptional circumstances, provided that the employee has given express consent to the monitoring. Note that general consent for a workplace monitoring policy is not sufficient to allow the employer to monitor personal content unless specific agreement was provided by the employee. Needless to say, an employer cannot monitor a private email account under the exclusive ownership of the employee. Regardless of the other meanings of a violation of an employee's right to privacy, if the employer discovers evidence due to an infringement of an employee's right to privacy, such evidence may not be admissible in a court of law.

As opposed to a proactive monitoring carried out by an employer on its employees, if an employer was accidentally exposed to an open private email message, the rule might differ. In a judgment given in May 2016, the Israeli Supreme Court determined that in the event of an accidental and passive exposure of a private email message, as opposed to an intentional monitoring without the prior approval of the court (the court did not discuss such a case), there is no justification to require the employer to receive a judicial order and the employer may use such an email message to protect its legitimate interests. Accidental exposure to an email message that provokes only a vague suspicion of infringement of a legitimate interest of the employer (as opposed to a message that clearly shows such) is not enough to establish protection under the law and such message will not be admissible as evidence in court.

In addition, under the PPA's guidelines, the use of surveillance cameras in the workplace must be only for legitimate purposes. The employees' explicit consent for the use of the cameras must be obtained, a clear and detailed policy regarding the use of the

cameras must be presented to the employees, private areas may not be filmed, and the use of footage for reasons differing from the predetermined purpose is prohibited.

Furthermore, in 2017, the Israeli National Labor Court ruled (in the Qalansawa Municipality case) that the use of a biometric system for monitoring attendance harms employees' right to privacy and to autonomy. Consequently, an employer's right will only overrule employees' rights to privacy if required by law or with the employees' free-willed and specific consent.

8. Scope of Telecommunications Regime

The law refers to wireless communication products as a "wireless telegraph" under the Ordinance of the Wireless Telegraph 5733-1972 (Wireless Telegraph Ordinance) and defines this as any method of communication through devices that transmit or receive information, communications, messages, or other signals through the use of electromagnetic wavelengths and without the help of a connector wire between the receiver and transmitter.

The creation, maintenance, activation, and installation of wireless devices requires a licence under the law. The Minister of Communications may establish exemptions to the need for a licence. The Director of Radio Wavelengths in the Ministry of Communication has the power to exempt a wireless device from the licence requirement if he or she believes that a licence would be unreasonable under the circumstances, as long as the device does not disrupt or disturb the use of other wireless devices.

Not every type of wireless communication product may be imported to Israel. Those that may be imported, per the Wireless Telegraph Ordinance, and that are not exempt require approval, either "suitability approval" or "type approval".

Suitability approval means that the wireless product meets the conditions set by the Ministry of Communication for wireless devices. These conditions involve defined assigned frequency bands and specific MHz output. Suitability approval can also be used to release certain wireless devices from customs for a set time period (usually five years).

Type approval means approval from the Ministry of Communication for certain wireless devices that enable efficient utilisation of radio frequencies and which do not disrupt or disturb the use of other wireless devices. One condition to market equipment that receives this approval type is that the individual who receives the device has a valid licence to activate the equipment. This approval can also be used to release certain wireless devices from customs for a set time period (usually five years). This approval type does not allow the activation, storage, or sale of the equipment; such activity requires separate licences from the Ministry of Communication.

A topic gaining a lot of attention is fifth-generation wireless technology (ie, 5G) in Israel. In July 2019, the Ministry of Communication published a long-awaited tender for the construction of fifth-generation mobile networks, offering government incentives worth ILS500 million (USD140 million) to winning bidders. Fifth-generation cellular network technology, 5G, touts surfing speeds approximately 20 times faster than current 4G networks. This innovative technology facilitates much faster information transmission than today's rates.

The entry of this new 5G technology will kick off the smart digital revolution that will affect all aspects of our lives: smart homes, smart cities, education, autonomous vehicles, advanced industry, and more.

As of today, the tender has been postponed for the third time, so we must wait to see what happens next with the fifth generation in Israel.

9. Audio-Visual Services and Video Channels

Licensing requirements apply to all terrestrial TV broadcasts, except if broadcasted over the internet. This issue is regulated under the Israeli Communication Law (Telecommunications and Broadcastings), 5742-1982 (Communication Law). In order to broadcast satellite television, which is primarily intended for the public in Israel or to a part thereof, a licence from the Minister of Communications (Minister) is required. Broadcasting and licences are regulated by a number of regulators, depending on the type of licence held. The Second Authority for Television and Radio is the Israeli commercial television and radio authority, the Cable and Satellite Broadcasting Council regulates cable-based and satellite-based telecommunication activities and broadcasts, and Kan – the Public Broadcast Corporation – focuses on public broadcasts.

Under the Communication Law, several preliminary minimal requirements must be met to receive a satellite broadcasting licence: (i) the applicant must be an Israeli citizen, an Israeli resident, or a corporation registered in Israel; and (ii) the applicant must not have been convicted of an offence that due to its severity or circumstances prohibits him or her from receiving a licence. In the case of a corporation, none of its directors or interested parties may have been convicted of such an offence.

There are several more considerations the Minister should address, as listed in the Communication Law.

In addition, the Minister shall consider:

- the financial and organisational capacity of the applicant;
- the professional experience of the applicant;
- the variety of broadcasts and services offered by the applicant; and
- the technology used by the applicant for broadcasting.

The fees for a broadcasting satellite licence, according to the Communication Regulation (Telecommunication and Broadcasting) (Television Broadcasting via Satellite) (License Fee and Royalties), are ILS30 million, approximately USD8,645,362.

Any entity wishing to broadcast radio in Israel requires a broadcast licence from the Ministry of Communication. According to the Communication Law, the Minister shall take into account the following considerations:

- the Israeli government's policy with respect to telecommunication and broadcasting to the public;
- public welfare considerations;
- the suitability of the applicant to broadcast satellite broadcasts; and
- the contribution of granting the licence to competition in the field of telecommunication and broadcasting.

There are several additional general laws that regulate broadcasting:

- the Classifying, Marking and Prohibiting Harmful Broadcasts, 5761-2001, which regulates the obligation to classify and mark television broadcasts that are not appropriate for children and teenagers;
- The Television Broadcast Law (Subtitles and Sign Language), 5765-2005, which regulates the integration of subtitles and sign language for the benefit of the deaf and the hearing impaired – the obligations under this law are imposed gradually;
- The Law to Limit the Volume in Commercials, Trailers and Other Broadcasts, 5768-2008, which regulates the volume levels allowed to be used in such broadcasts as mentioned above;
- Equal Rights of Persons with Disabilities Regulations (Accessibility to Telecommunication Services); and
- Relief for the Deaf Law, 5752-1992.

Existing requirements for audio-visual service do not apply to online video channels, as online video channels have yet to be regulated under Israeli law.

10. Encryption Requirements

Encryption is regulated by the Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974 (Encryption Order). Based on a 1998 amendment to the Encryption Order, the control and licensing of encryption items were transferred "from a military to a civilian licensing authority, i.e. from the IDF to the Ministry of Defense".

The Encryption Order prohibits any person from engaging in encryption in the absence of a licence issued by the General Manager of the Ministry of Defense and in violation of the conditions enumerated in the licence. This requirement is broader than the export control regimes applied to encryption in a number of other jurisdictions.

A person or entity may use encryption items for its personal use without the licence, provided that: (i) the encryption item is not delivered to any other person or entity; and (ii) the encryption item was purchased from a licensed Israeli entity or person, or the encryption item was downloaded from the internet for personal use for data security or electronic signature.

For any use other than personal use, a person or entity that desires to develop, import, or export encryption items, including downloading encryption items for implementation in its product, must hold a valid licence.

The General Manager of the Ministry of Defense is authorised to enter any place where encryption-related activity is being conducted and to request a licensee to provide information at any time before or after the issuance of an encryption licence.

The Encryption Order provides for three categories of licences for engaging in encryption:

A "restricted licence" imposes restrictions on engagement in encryption items. These restrictions may also apply to permissible forms of engagement in encryption items, or to the nature of permissible sales (eg, restriction on selling to certain countries and sectors). As a rule, a restricted licence is valid for one year.

A "special licence" is for specific engagement, generally involving a sale to clients who do not fall under the restrictions imposed on an applicant for a restricted licence. As a rule, a special licence is valid for one year.

A "general licence" is for a particular encryption item that allows the licence holder free use of that item (other than modifications or integration that essentially create a new item, for which a separate licence is required). The sale of such encryption items is decontrolled (ie, deregulated) and not subject to reporting

procedures. Such general licences are issued with no time limit to their validity.

The Encryption Order also provides for a category of "free means", which exempt certain encryption activities from licensing requirements. "Free means" are defined as "means of encryption for which a general licence has been granted or which the Director-General has declared to be decontrolled". Once an encryption item is defined as a free means, it is free of the licensing restrictions. A periodically revised list of encryption items that have been declared "decontrolled" is published in the Official Gazette of the Israeli government as well as on the Ministry of Defense website.

On 24 September 2019, the Ministry of Defense announced that it is debating regulatory easements for hundreds of software and cyber-companies who encrypt and sell their products worldwide. These easements will be given as a result of the changes being made to the Encryption Order, according to which any company that deals with cryptographic measures must obtain approval from the Israeli Defense Export Controls Agency prior to any export transaction.

The regulatory easements require legislative changes and the approval of the Knesset Foreign Affairs and Defense Committee. Therefore, they will only be applied in the next Knesset.

A person is exempt from applying for a licence for engagement in commercial encryption items subject to the following conditions:

- the product or encryption items were purchased from a licence holder for sale and distribution of commercial encryption items;
- the product or encryption item was "downloaded" from the internet for personal use for data security or electronic signature.

Barnea Jaffa Lande & Co is one of Israel's leading commercial law firms, with an esteemed reputation in the international arena. About 70% of the firm's activities have international aspects. Barnea Jaffa Lande & Co's international capabilities, which include commercial knowledge, innovative thinking, and a broad network of relationships with foreign law firms and industries, enable it to respond to clients' needs in all spheres of its business activity. The firm provides legal counsel in a variety of fields, including corporate law, M&A, infrastructure, litigation, technology, internet, real estate, banking and finance, capital markets, white collar, employment, tax, internet, regulation, and specialised focused sectors.

Authors

Michael (Micky) Barnea is the managing partner at Barnea Jaffa Lande and boasts over 25 years' experience advising cross-border clients in the high-tech sphere. Micky counsels a variety of early-stage and late-stage companies, as well as leading venture capital, corporate venture, and private equity investors. He also manages prominent cross-border technology-related transactions. Micky assists high-tech clients in a variety of industries, including fintech, artificial intelligence, life sciences, internet, financial services, and advertising. He is a well-known figure in the Israeli high-tech ecosystem, lecturing on a regular basis to various Israeli accelerators and incubators, in addition to serving as a mentor for young entrepreneurs.

Daniel Lorber is a partner at Barnea Jaffa Lande. He possesses extensive experience representing companies in a wide range of international commercial transactions, with an emphasis on mergers and acquisitions, financing transactions, and sophisticated technology transfer arrangements. Daniel provides counsel in a variety of commercial matters, including technology licensing transactions, domestic and international R&D grants, distribution and manufacturing agreements, capital raising, complex joint ventures, sales of assets, and privacy protection. He also counsels start-ups, technology companies, and senior managers on all aspects of designing and implementing capital incentive plans and individual grants for employees and senior executives.

Anat Even-Chen is a partner at Barnea Jaffa Lande, leading the regulation team. She possesses vast experience in providing legal counsel on various regulatory issues, including privacy and personal data, financial regulation, environmental regulation, and antitrust matters. Anat offers particular expertise in advising a range of clients on technology and privacy law. She is well-versed in data sharing, data protection laws in Israel and Europe (GDPR), and database and cyber-related matters. An integral part of Anat's technology practice is advising clients on the cyber-protection and privacy law issues applicable to their business models, including the cross-border aspects of their activities.

Nir Abraham advises public and private corporations on the various legal aspects of their activities, with a focus on corporate, commercial, and technology-related issues. Nir provides ongoing legal counsel to companies on a wide range of activities, including mergers and acquisitions, raising capital, intellectual property, and distribution, franchise, licensing, and manufacturing agreements.

Barnea Jaffa Lande & Co

58 Harakevet St.
Tel Aviv
Israel

Tel: 972 3 6400600
Fax: 972 3 6400650
Email: mail@barlaw.co.il
Web: www.barlaw.co.il

BARNEA