International Bar Association Series

VOLUME 26

Introduction, Contents & Editor

In partnership with the International Bar Association, Kluwer Law International publishes a wide variety of books covering various aspects of legal practice and policy. Recent titles cover areas such as corporate governance, directors' liability, employment law, and competition law. Each volume is edited by a leading practitioner, with contributions from law firms around the world.

Objective & Readership

Practitioners

The titles published in this series are listed at the end of this volume.

Social Media and Employment Law

An International Survey

Edited by

Anders Etgen Reitz
Jan Rudolph
Philip M. Berkowitz

International Bar Association Series

Wolters Kluwer

Published by:
Kluwer Law International
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
Website: www.wklawbusiness.com

Sold and distributed in North, Central and South America by:
Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America
Email: customer.service@aspenpublishers.com

Sold and distributed in all other countries by:
Turpin Distribution Services Ltd
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom
Email: kluwerlaw@turpin-distribution.com

Printed on acid-free paper.

ISBN 978-90-411-4768-4

Printed and Bound by CPI Group (UK) Ltd, Croydon, CR0 4YY.

International Bar Association

The Global Voice of the Legal Profession

The International Bar Association (IBA), established in 1947, is the world's leading organisation of international legal practitioners, bar associations and law societies. The IBA influences the development of international law reform and shapes the future of the legal profession throughout the world.

It has a membership of over 55,000 individual lawyers and 206 bar associations and law societies spanning all continents. It has considerable expertise in providing assistance to the global legal community as well as being a source of distinguished legal commentators for international news outlets.

Grouped into two divisions – the Legal Practice Division and the Public and Professional Interest Division – the IBA covers all practice areas and professional interests, providing members with access to leading experts and up-to-date information.

Through the various committees of the divisions, the IBA enables an interchange of information and views among its members as to laws, practices and professional responsibilities relating to the practice of business law around the globe.

Employment and Industrial Relations Law Committee

The aims of the committee are to develop and exchange knowledge of employment and industrial relations law and practice. Members support each other through the provision of innovative ideas and practical assistance on day-to-day issues. In addition,

through its journal and through presentations, conferences, the committee ensures the dissemination of up-to-date law and practice in this highly important business area.

International Bar Association Global Employment Institute

The IBA Global Employment Institute (IBA GEI) wasformed in early 2010 for the purpose of developing for multinationals and worldwide institutions a global and strategic approach to the key legal issues in the human resources and human capital fields.

Drawing on the resources and expertise of the IBA membership, the IBA GEI will provide a unique contribution in the field of employment, discrimination and immigration law, on a diverse range of global issues, to private and public organizations throughout the world. The IBA GEI is designed to enhance the management, performance and productivity of these organizations and help achieve best practice in their human capital and management functions from a strategic perspective.

The IBA GEI will become the leading voice and authority on global HR issues by virtue of having a number of the world's leading labour and employment practitioners in its ranks, and the support and resource of the world's largest association of international lawyers.

CHAPTER 16
Israel

Ofer Ravid & Revital Shprung-Levy

§16.01 INTRODUCTION

In Israeli law, the right to privacy ranks high in the normative hierarchy, being a constitutional supra-statutory right, which is among the most fundamental human rights in Israel. The right to privacy was established in Basic Law: Human Dignity and Liberty, which prescribes a general provision in section 7 thereof, that every person is entitled to privacy and freedom from public scrutiny. Furthermore, the right to privacy and the protection of information about a person is also established in a specific statute, the Privacy Protection Law, 5741-1981 (the '*Privacy Protection Law*'), the infraction of which may amount to a criminal offence or a civil tort.

Rules concerning privacy protection in general and personal information in particular, are dispersed throughout dozens of additional Israeli statutes, such as the Criminal Register Law,[1] the Communications Law,[2] the Genetic Information Law,[3] the Patient Rights Law[4] and numerous others.

Recognition by the governmental authorities of the State of Israel of the great importance of a person's privacy and the need to protect it led to the foundation of the Israeli Law, Information and Technology Authority ('*ILITA*') by the Ministry of Justice in 2006, which is entrusted with the protection of personal information in Israel. As such, ILITA represents the State of Israel in the international arena of personal data protection and promotes international cooperation, within which, among other things, ILITA represents the State of Israel in international committees and projects (such as the ICCP, WPISP, OECD and Twinning).

1. The Criminal Register and Rehabilitation of Offenders Law, 5741-1981.
2. The Communications Law (Bezeq and Broadcasts), 5742-1982.
3. The Genetic Information Law, 5761-2000.
4. The Patient Rights Law, 5756-1996.

However, in the modern era, technological progress gives rise to new issues, including ones pertaining to privacy protection in social media, which Israeli law has not yet addressed.

In this article, we shall focus on privacy protection in the workplace from the perspective of social networks. It is noteworthy that Israeli law has chosen an approach that expands recognition of the employee's right to privacy at the workplace, with an inclination toward the common concepts in European law and the values thereof, as opposed to the American approach. However, case law in respect of privacy protection in the workplace is still sparse and does not address the use of social networks.

In examining privacy protection in the workplace, the starting point for the Labor Courts is a set of balances between conflicting rights. On the one hand, the rights of the employee to personal autonomy, dignity, privacy and anonymity, and, on the other hand, the employer's legitimate interests and his requirement of comprehensive information about the employee in all areas of his life, as a condition for hiring, during the performance of the work and for the purposes thereof. Neither of the rights are absolute, hence the legal system's need to achieve balances between conflicting rights, using fundamental concepts of Israeli labour law, such as good faith in employment relations and the lack of equality between the employee and employer.[5]

§16.02 USAGE OF SOCIAL MEDIA BY EMPLOYERS (TO COLLECT INFORMATION ON THE EMPLOYEE)

[A] General Regulations on the Usage of Social Media under Data Protection or Privacy Laws in the Country

Specific legislation addressing the use of social networks and the collection of information through social networks from the perspective of data protection or privacy protection has not been enacted in Israel yet.[6]

5. Of privacy at the workplace, see L.C.H. 4-70/97 *Tel Aviv University v. the General Federation*, PD L 385 (the '*University Judgment*').
6. There are statutes that specifically address offences, also if committed via computer and internet. Thus, it is noted, for example, that the Prevention of Sexual Harassment Law, 5758-1998 (the '*Sexual Harassment Law*'), also expressly prohibits harassment via computer and computer material. This law focuses on sexual harassment in the workplace. Under this law, an employer must take reasonable measures to prevent sexual harassment or persecution in the framework of the employment relations by an employee or a person appointed by the employer. Moreover, there is legislation that also has indirect implications on social network activity, such as the Defamation Law, 5725-1965, which defines 'Defamation' as something the publicity of which may humiliate a person in the eyes of others or make him the object of hate, scorn or ridicule. Publicity, for the purpose of defamation, is any publicity, whether oral or written or in print, which was intended for a person other than the injured party and came into the hands of such person or another person other than the injured party. Undisputedly, social networks are a fertile ground for publicity (regrettably also offensive publicity) and the speed at which information is conveyed through them might constitute defamation. Israeli courts have identified the uniqueness of social networks as pertains to responses and publicities therein in terms of defamation, and, in view of the absence of a revision of the defamation law, have created modifications and required adjustments.

The Israeli legislator has acknowledged the need to regulate the manner of use and of information and the protection thereof in specific legislation.[7] The principal and pertinent statute for the protection of privacy in respect of information is the Privacy Protection Law, which includes a special arrangement concerning databases and a special arrangement concerning the transmission of information between public entities.

Under the Privacy Protection Law, a person shall not invade the privacy of another without his consent. An invasion of privacy includes, *inter alia*, the following acts: 'photographing a person when he is in the private domain', 'publicizing the photograph of a person under circumstances in which the publicity might humiliate or degrade him', 'publicizing or conveying something obtained by way of invasion of privacy', 'use of information regarding a person's private affairs or conveyance thereof to another, other than for the purpose for which it was conveyed' and 'copying of the contents of a letter or other document which was not intended to be publicized, or the use of its contents, without permission from the addressee or the writer'.[8] Although the Privacy Protection Law does not explicitly refer to social media, distribute information through social media without consent may be deemed as invasion of privacy

Collecting information on a job candidate or employee without consent may even expose the employer to additional potential claim of discrimination and breach of Equal Opportunities in Employment Law, 5748-1988 (the '*Equal Opportunities in Employment Law*') or the Equal Rights for Persons with Disabilities Law (the '*Equal Rights for Persons with Disabilities Law*'), 5758-1988.

[B] Collection Prior to Hiring

Israeli law contains no explicit prohibition against employers' collecting information about a job candidate through social networks. However, surveillance on potential employees on protected social networks may cause a material injury to the candidate's privacy. The reason therefore is that even seemingly 'innocent' surveillance may expose a lot of information about the person's personality and habits, which are not necessarily relevant to his hiring and/or to his/her work.

The authors believe that publicity through social media that is available to any and all is no different than publicity in the town square, the expectation to privacy may be lower, and therefore may have fewer restrictions. Social media that is available to any and all should be distinguished from 'protected' information on social media (e.g., that entering into such social media requires a password). In this section, we will refer to protected information on 'protected social media'.

The legislator and labour courts are yet to address whether an employer may request the password to a social network from a job candidate. Thus, under the current legal regime, an employer is not legally prohibited from requesting the password or the acceptance of a friend request on a social network. That differs from the prohibition

7. This goes beyond the general protection of a person's privacy by means of Basic Law: Human Dignity and Liberty (as mentioned in the previous section).
8. If the document is not of historic value and it has not been fifteen years since it was written.

that Israeli law imposes on employers with respect to posing certain questions to a job candidate.[9]

However, according to present case law, an employer's request for a job candidate's personal password for the purpose of accessing protected personal information may be deemed disproportionate and might even expose the employer to potential future lawsuits including breach of anti-discriminations laws (as shall be described below).

Under the Basic Law: Human Dignity and Liberty, entering a person's private domain without his consent constitutes an invasion of the person's privacy. The case law recognized the private virtual space of the computer user as equivalent to the personal physical space. Thus, unauthorized access to the private virtual space violates a person's constitutional right to privacy.

The Privacy Protection Law also includes a consent condition. According to the Privacy Protection Law, consent means 'informed consent', i.e., that the person consenting to the invasion of privacy has the information that is reasonably required to enable him to decide whether or not to consent. Therefore, the prior, informed consent requirement mandates unconditional disclosure and full transparency by the employer in respect of the nature of the surveillance and the use to be made of the information collected. Furthermore, the collection of an informed consent from a job candidate should be based on the principles of Israeli law, which are: collection of the information for a worthy purpose, legitimacy, transparency, proportionality, restriction of the purpose[10] and good faith.

In view of the situation where the job candidate is aware of the fact that his refusal to consent might jeopardize his being hired, the candidate's decision to allow or disallow the employer's information search in the context of the considerations for his hiring is not always given 'voluntarily'. Hence, under these circumstances, the court may rule that even if the employee's informed consent is given, the presumption is that it is not voluntary but forced, and is thus invalid. Insofar as the employer argues otherwise, the burden of proof for refuting such presumption rests with him.

As mentioned above, by collecting information on a job candidate, the employer runs the risk of additional potential lawsuits, *inter alia*, by virtue of a potential claim of violation of the anti-discrimination laws, such as Equal Opportunities in Employment Law, or the Equal Rights for Persons with Disabilities Law. In the framework of the

9. Information which is not to be requested from a candidate or an employee includes, among others, genetic information, questions regarding criminal records, questions pertaining to IDF medical profile.

10. The principle of legitimacy means considering whether surveilling a job candidate on social networks is done for a worthy purpose or a legitimate interest concerning the needs of the job. The principle of proportionality concerns the proportion between the benefit of carrying out the worthy purpose of the policy of surveilling a job candidate and the damage of and infringement on the job candidate's rights to privacy and dignity, personal autonomy and anonymity as a result of the surveillance policy, as aforesaid. In terms of the principle of proportionality, we shall examine whether the surveillance by the potential employer is excessive and whether there are less intrusive measures that could have been taken instead. The principle of proportionality examines whether the information's recipient uses the information provided to him for a specific legal purpose and for it alone.

aforesaid laws, an employer is prohibited, among other things, from discriminating against job applicants in the process of their hiring on grounds of their gender, sexual orientation, personal status, pregnancy, fertility treatments, IVF treatments, parenthood, age, race, nationality, country of origin, views, political affiliation or military reserve service, summons to military reserve service or anticipated military reserve service.

Under the Equal Opportunities in Employment Law, when an employer directly or indirectly requires information from a job candidate on an issue in respect of which discrimination is prohibited, he will be obligated to prove that he did not discriminate against the candidate.

In Sharon Plotkin,[11] Sharon was a female candidate who was informed during her hiring interview by the prospective employer that there were two jobs available. Ms. Plotkin expressed a wish to work in one of them, an outside sales person position, due to the improved employment conditions of this job. However, she was told unequivocally that women are not suitable for this position, mainly due to the long hours required outside the office. The labour court determined that behaviour was unacceptable, regardless of the employer's intent or motivation. Rather stereotypical character questions during a personal interview can create liability on a prospective employer. Moreover, when necessary skills are better suited for men than for women, the employer has to prove that such need is indeed necessary for the job, and that an employer cannot settle for less. It is further clarified that the Privacy Protection Law is not more lenient when the collection of information on a job candidate or an employee is performed through third parties (such as placement or screening agencies). In the framework of the Privacy Protection Law, the overall liability lies with the employer and he is required to examine whether the collection of information is in accordance with the principles mentioned above.

[C] Collection during Employment and Thereafter

Israeli legislation has yet to expressly address restrictions on employers in the process of collecting information about employees through social networks.[12] The principles stated in respect of the protection of the privacy of a job candidate are also applicable to the collection of information on the employee during employment and thereafter. The requirement of pursuing a legitimate purpose with proportionality, restriction of the purpose and good faith mandate that the collection of information from an employee be done solely for legitimate purposes, which are related to the employment relations, and whether the surveillance by the employer is excessive and whether there are less intrusive measures that could have been taken instead.

11. L.C.H. 3-129/99 *Sharon Plotkin v. Isenberg Brother Ltd.*, PD LG 481.
12. The Privacy Protection Law, includes provisions with respect to data management in a computerized data system by an employee (which regulates the protection of the collected data).

It should be noted that in 2008, a general collective bargaining agreement was registered,[13] (the '*CBA*') which governs the obligations and rights of employees and employers with respect to computer use and rules of conduct for the workplace, wherein the employee uses the employer's computer, but the CBA does not specifically address social networks.[14]

In *Re Iskov,*[15] the National Labor Court discussed for the first time the issue of employees using an employers' computers, information technologies and e-mail correspondence in the workplace and the employees' right to privacy in the context of such use. The judgment establishes the rights and duties of the employer and employee with respect to computer and e-mail use in the workplace and balances the employee's right to privacy and the employer's right to manage his business as he pleases, while protecting his property. It was ruled, *inter alia*, that an employer shall set a clear policy on the permitted and prohibited computer uses at the workplace according to legal rules, including the duties of good faith, loyalty and fairness and in view of principles of transparency, proportionality, legitimacy and attachment to the purpose. As the National Labor Court has set clear boundaries in the *Iskov* case regarding the employer's monitoring of employees' personal e-mail correspondence and restricted permissible monitoring to a specific and unusual set of circumstances (such as illegal or criminal activity), it is safe to assume that the Labor Courts shall take a similar stance regarding the employers' monitoring of personal information found on social networks without the employees' prior consent.

Recently, in *Anna Gorlik,*[16] the Regional Labor Court ruled that in the event that an employer was exposed to employee's correspondence on the employee's Facebook page, although the employee left the Facebook open on the computer at work, the employer is not allowed to print, share or copy such information. In such a case, the Labour Court determined that the employer who collected information through the employee's Facebook page and shared it breached the employee's right to privacy.

[D] Co-determination Rights?

Generally, the consultation duty may serve as a foundation for a mechanism requiring an employer to seek prior approval from third party (e.g., employees' committee, or employees' organization at workplaces having collective employment relations, in accordance with the provisions of collective bargaining agreements). However, since Israeli law does not address social networks, there is consequently no legal duty to hold

13. The CBA is between the Histadrut, New General Federation of Labor and the Coordinating Bureau of the Economic Organizations. Collective Bargaining Agreement, No. 20087033.
14. The CBA includes a statement by the parties of their intention to apply to the Minister of Industry, Trade and Labor (currently the Minister of Economy) with a request that an expansion order be issued, applying the provisions thereof to all employers and employees in Israel. However, as of the date hereof, such expansion order has not been issued yet.
15. L.A. (National) 8/90 *Tali-Iskov Inbar v. the State of Israel – the Commissioner of Women's Labor et al ('Re Iskov')*.
16. L.D (Tel-Aviv) 2909-05-12 *Anna Gorlik v. the State Iliya Anbindar ('Annav Gorlik')*.

such or other consultation before collecting information on employee/candidates through social media.

[E] Any Regulatory Issues?

Rules concerning the protection of privacy in general and the protection of personal information in particular are dispersed throughout dozens of additional Israeli statutes, but still without reference to collection information through social media. In this chapter, we shall present the principal statutes containing aspects related to employment relations:

The Criminal Register and Rehabilitation of Offenders Law, 5741-1981: a printout of the criminal register includes an individual's criminal record. The printout is intended solely for perusal by the person to whom the information refers or for perusal by persons authorised under law thereto. An employer is prohibited from demanding to receive a copy of an employee's or a job candidate's criminal record.

The Genetic Information Law, 5761-2000: an employer is prohibited from demanding genetic information, or the undergoing of genetic testing, from an employee or a job candidate, for any purpose, including hiring, employment conditions, or dismissal. If an employer demands of an employee to provide genetic information or undergo genetic testing in violation of the provisions of the law, and the employee refuses to do so, the employer is forbidden to make choices related to hiring, promoting, employment conditions, or dismissal that are disadvantageous for the employee due to the employee's refusal. However, this prohibition does not apply to workplaces in respect of which the Minister of Health has determined that genetic testing is necessary for reasons of protecting employees' health.

The Patient Rights Law, 5756-1996: the law governs the rights of the patient, and, *inter alia*, sets forth his right to privacy in all stages of the treatment and the retention of information pertaining to his treatment.

The Equal Rights to Persons with Disabilities Law: under this law, an employer is prohibited from discriminating between employees or job candidates due to their disabilities, insofar as they are competent for the position or office in question.

The Equal Opportunities in Employment Law: under this law, an employer is prohibited from discriminating between employees or job candidates due to their gender, sexual orientation, personal status, pregnancy, fertility treatments, IVF treatments, parenthood, age, race, religion, nationality, country of origin, views, political affiliation or military reserve service, summons to military reserve service or anticipated military reserve service.

§16.03 USAGE OF SOCIAL MEDIA BY EMPLOYEES

[A] Rights and Duties of Employees

As previously noted, the Israeli legislator has yet to prescribe provisions with respect to use of social networks. Such duties apply to employees by virtue of the general law, including the employee's duty of loyalty to the workplace. The starting point is that an employer may require an employee to 'surf' the internet for work purposes, and we

shall thus devote this chapter to the legal aspects arising from an employee's 'surfing' social networks for personal purposes during his work.

[1] Right to Use Social Media at the Workplace

As of yet, no law has been enacted with respect to employee's 'surfing' social networks during working hours. In *Re Guri,*[17] the Labor Court ruled that an employee who 'surfed' the internet for multiple hours for private purposes, in contrast with the instructions of his supervisors, entered improper websites and conducted surveys online for personal purposes, committed a severe disciplinary violation. The Court deemed that by such acts the employee harms the workplace. Furthermore, the fact that other employees at the same workplace behave in the same manner does not constitute an adequate defence for the employee. In *Re Suhil Halon*[18] it was ruled that surfing on the internet for private purposes rather than for work purposes constitutes a clear disciplinary offence. However, the Court ruled that the proportionality of the penalty should be examined according to the circumstances, including the extent of the surfing, the rules on surfing at the workplace, the damage incurred by the employer as a result of the surfing and the balance of the interests of the employee and the employer.

The CBA reflects the balance between the rights of the employer and 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.

[2] Protection against Misuse by Peers/Cyber Bullying at the Workplace?

Israel has not yet enacted a law that protects employees from bullying or cyber bullying through the network, but, as noted above, there are a few unique protections including, bullying that constitutes defamation, invasion of privacy and sexual harassment.[19] Bullying by the employer may be considered a breach of the employment agreement or at least a lack of good faith in the existence of a contract entitling the employee to damages. It should be noted, however, that the labour courts have only awarded damages for mental distress in extreme cases. Furthermore, bullying after commencement of employment or intensification of bullying, may allow the employee to resign under circumstances that entitle the dismissed employee to severance pay.[20]

17. M.C.M. 2250/01 *Guri v. the City of Ramla*, PDL JJ 55 ('*Re Guri*').
18. M.I. 3125/08 *Suhil Halon v. the Fund for Medical Research, Infrastructure Development & Health Services near the Rambam Medical Center*, (Dated 18 December 2008) ('*Re Suhil Halon*').
19. See *supra* note 6.
20. According to Israeli law, generally a dismissed employee, as opposed to a resigning employee, is entitled to severance pay. However, the law has recognized special circumstances entitling the resigning employee to severance pay as well. In this context, it is worth noting that section 11 of the Severance Pay Law states that an employee who resigned due to substantial deterioration of

[3] Duties of Employees

The duties of an employee to his employer with respect to use of social networks, either for personal or work purposes, are subject to the duties of an employee to his employer under the employment agreement, the workplace policy and the general law.

The employee's duty of loyalty to his employer and the duty of good faith are noteworthy in the context of duties of employees under general Israeli law.

In the framework of these duties regarding the use of social media, the employee is required to refrain, *inter alia*, from writing contents that directly or indirectly expose a trade secret of the employer or impair the reputation of the company, its clients or its employees, either at his private time or during working time.

[a] Private Use and Business Use of the Employee

As mentioned above, the employer may restrict the employee's use of social media during working hours. However, generally, an employer has no responsibility for statements made by employees in their personal lives outside of the workplace, and is not allowed to spy on them or interfere with their lives outside the workplace. Therefore, for example termination of an employee due to publishing his personal opinion (such as political views) through social media may expose the employer to discrimination and unlawful dismissal claims.

In *Abir Ruashda,*[21] an employee was dismissed after sharing with her friends on her Facebook page, her political views through her private account. The employee filed a temporary injunction to prevent her dismissal based on the ground that she was being discriminated against due to her personal views. The employer claimed that since the employee's Facebook included her place of work, by publishing such political views, the employee crossed the boundary of personal space. In addition to this, the employer claimed that the employee's political views negatively affected the employer's reputation. The Labour Court ruled that an employer shall not discriminate due to personal views of his employees and ruled to return the employee to work until a decision was reached in the main proceeding. The Labour Court rejected the employer's claim that the employee's political views affected the employer's reputation since the employee shared her personal political views only with her friends and there was no evidence to connect the employee's political views to her place of work.

Nevertheless, employees may at the employer's request be required to use social networks as a working tool for work purposes. As long as these requirements as mentioned above are consistent with the general law, this would be done within the framework of the employee's obligations towards the employer for the purpose of performing the job.

---

employment conditions or other circumstances where the working relationship does not require the employee to continue to work, is entitled to severance pay.

21. L.D.J 26396-08-014(Nazareth) *Abir Ruashda v. Mor Mar Ltd*.

[4] What Can Employers Regulate?

In *Re Iskov*, it was noted that an employer should implement a clear policy with respect to the allocation of virtual space in computer in the workplace. In setting the policy on allocation of private virtual space in the workplace, considerations such as the following may be taken into account: the nature of the workplace, its character, its operations and special needs in general; the type of work performed by the employee, the character of the position he fills and the nature thereof. There may be cases in which use of information technologies for personal purposes is completely banned from the workplace, if there are legitimate interests of the employer's, such as considerations of security and data protection, which stem from the nature of the workplace and the nature of the employee's occupation or position.

The employer must inform the employees of the policy on use of the technologies available to the employees for work purposes. In the framework of the policy practiced at the workplace and subject to the principle of transparency, the employer may prohibit the employees from accessing certain websites, set a time frame for surfing websites, or/and forbid uploading of external data such as videos. Furthermore, the employer may put technologies in place for blocking improper computer use by employees. Such employer's instructions and guidelines to the employees shall be subject to the principles of good faith, disclosure, transparency, legitimacy, proportionality and connection with the purpose.

Thus, the CBA too provides that an employer has the right to determine rules on use or non-use of computers in the workplace. The rules of use will be aimed at realizing the business's objectives and serving a worthy purpose. The employees must be informed of the rules of use, and the rules shall be consistent with the spirit of the CBA and the law.

Therefore, in order to protect employees in the workplace on the one hand, and protect employers' properties on the other hand, we recommend that Israeli employers draft a clear policy for computer use, which includes, *inter alia*, restrictions on use of the company's computer, internet (including social media), or e-mail for inappropriate or unsuitable purposes, including surfing inappropriate or unsuitable websites (such as websites containing pornographic content and so forth), installing software, and transmitting material that is unrelated to work or that might harm the company, its clients, other employees or any third party.

[B] Monitoring and Gathering?

As mentioned above, *Re Iskov* is the leading precedent that determined the rules for the monitoring of employees' e-mails by their employer. The Court drew a material distinction between two main types of virtual e-mail accounts that are available for the employee's use: an account owned by the employer and an account owned by the employee.

Insofar as an e-mail account is owned by the employer, this can be divided into: (i) a professional account designated solely for work purposes and where personal use

is forbidden for the employee; and (ii) dual and personal accounts allotted by the employer for the personal needs of the employee at the workplace.

The employer may monitor communications data and enter content data when dealing with a professional account solely for work purposes, including the professional e-mail correspondence therein. However, even if the employee has exchanged personal correspondence in the professional account *in contrast with the policy* of the workplace, the employer may not enter the content data of such personal correspondence. This can only be done where exceptional conditions justify accessing such content data in view of the principles of legitimacy, proportionality and applicable law, and insofar as the employer sought and received in advance the explicit informed voluntary consent of the employee thereto.

The employer may make an account available to the employee that is meant to serve his personal needs and personal correspondence. In this context, the employer may allow the employee to exchange personal correspondence in the account made available to him for work purposes in general, such account being referred to as a dual account.

Another option is to allocate a separate account to the employee, in which he is able to exchange personal correspondence, which is not related to the work and is not for work purposes, such account being referred to as a personal account.

The employer may not monitor personal correspondence exchanged by the employee, either in a personal account or a dual account. In addition, the employer is prohibited from accessing the contents of the personal correspondence, other than in exceptional circumstances.[22]

Upon fulfilment of the aforesaid cumulative conditions, the employer must seek and receive the employee's explicit, informed and voluntary consent to the general policy concerning the employer's access to the personal or dual account and the personal correspondence contained therein.

Furthermore, insofar as accessing a dual account is concerned, the employee's specific consent is required for any act of the employer's which enters the contents of his personal correspondence, as distinguished from his professional correspondence in the same account.

The employer may permit the employee's use of an external-private account owned by the employee for his private needs, on the virtual space of the workplace. In view of the employee's sole ownership of the external-private account, the employer is prohibited from monitoring communications data or content in respect of the employee's personal use of the private account, as well as prohibited from accessing the private account and the contents of the employee's e-mail correspondence contained therein. Insofar as the employer believes that the conditions that merit such acts and similar acts have been fulfilled, he is required to apply to the court and move for a suitable remedy in the form of an Anton Piller order (a court order in a civil proceeding that allows the plaintiff to seize exhibits and evidence held by the defendant, if there is

22. By virtue of the legitimacy principle and only after the employer takes less intrusive technological measures that attest to the employee's inappropriate use of the technologies made available to him for work purposes.

cause for concern that the defendant will conceal them during the trial), in order to be allowed to search and seize data from the employee's private account. As a rule, the order will be issued only in rare and exceptional cases and upon the fulfilment of the required conditions under law.

[C] Sanctions/Remedies?

[1] Employer-Side

Israeli law has not yet referred to the right of an employer to forbid employees' use of social networks. However, as mentioned above, the Labor Court has recognized unreasonable internet use by employees during working hours, for private purposes in violation of the employer's workplace rules, as a severe disciplinary breach. In light of the ruling, the proportionality of the penalty must be considered in each case, taking specific circumstances into account, including the extent of surfing, the rules on internet surfing in the workplace, the damage caused to the employer as a result of browsing, and the balance between employee and employer interests.[23]

Generally, an employer may dismiss an employee at its sole discretion and workplace needs, subject to the principles of good faith and fairness and a termination process including hearing. However, as mentioned above, dismissal solely due to the employee's expression of opinions may expose the employer to discrimination claims and unlawful termination.

Furthermore, Israeli law has recognized situations that deny the employee the right to severance pay and notice prior to termination.[24] However, it should be noted that the denial of severance pay is allowed by the court only in extreme cases. In this regard, all circumstances of the specific case must be examined, taking into account the severity of the damage caused to the employer, the advance notice required by other employees, the duration of the employment, the nature of the relationship between the parties over the years, the level of trust and reliability that existed between the parties during the period of employment, and the employee's contribution to the enterprise. In severe cases of employee damages through the use of social networks (e.g., exposure of trade secrets), the employer may seek payments.

23. See *Re Suhil Halon* (see *supra* note 18).
24. Sections 16 and 17 of the Severance Pay Law – 1963, regulate the denial of severance pay in two situations: when there is a collective agreement between the parties that set out disciplinary offences that justify the denial of severance pay, or when there is a collective agreement between the parties then the court may determine that circumstances exist which justify dismissal without severance pay. Section 10 of the Notice of Dismissal and Resignation Law – 2001, governs dismissal without notice in circumstances where the employee is not entitled to severance pay upon dismissal as mentioned above, or according to the decision of a Disciplinary Court.

[2] Employee-Side

Israel has not yet regulated the rights of employees in the event of prohibited use of the social network by an employer. An employee, who claims for injury to his privacy through the use of such prohibited usage of the social networks, may file a claim for monetary compensation, including compensation without proof of damage and compensation for non-pecuniary damage. It should be noted, however, that labour courts have not awarded damages for mental distress except for extreme cases.

§16.04 PROCEDURAL ISSUES?

[A] Litigation and Discovery

The authors believe that social media will have an increased presence in the Israeli courtroom, and not only regarding workplace. Social media can be filed as part of statement of claim, statement of defence and can be sought during discovery process.

[B] Usage of Illegally Obtained Data

Under the Privacy Protection law, information obtained during the invasion of privacy is unacceptable for use as evidence in court. The exception is the obtaining of the victim's consent. However, the court may allow the use of such information as evidence, by granting a temporary relief to discover information, despite its violation of one's privacy, as long as the injurer holds defence claims against the invasion of privacy claim or the privacy exemption in accordance with the law.