LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Controls from remote through Social networks

ALESSANDRA INGRAO
Università di Milano
alessandra.ingrao@gmail.com

1. The peculiarities of "identifying Social networks" and their potentialities to control from remote the employees' activities and behaviour.

«Not some time ago, in a far land, there was a system of feudal editors. These editors were attempting to control the wider number of users. Archaeologists would have defined this prehistoric age web 1.0. The users, for a short period, were happy, until the day when they discovered that also themselves could easily become editors too, and create their own communities and kingdoms. Therefore, they created a new land of democratic contents, where every user would have had the possibility to become king of himself. New sites allowed very soon users to publish their royal decrees (blog), to vote for their favourite contents, to find old friends, to become stars, to have followers and, in some cases, to become also most important than the older editors. The users called this new Utopia Web 2.0. Welcome in the Social web» (1).

The Social networks, during their overwhelming rise, went beyond the doors of factories, offices, and, in general, of working places. Web 2.0., by means of its many features, became one of numerous instruments of control from remote on the behaviour of the user-worker.

Two simple operations submit the worker to control while using Social networks: the creation of identifying profiles (publication of

(1) F. Mini, *Social Media. Introduction*, in R. Ford, J. Wiederman (edited by), *Internet Case Study Book*, Taschen, 2010, 232.

contents and customization) (2) and the active participation (interaction) to a virtual *societas*.

The web user leaves the depressing anonymity of his ordinary life and reveals to the administrator of the network and to other users his own identity, his preferences (like), his opinions (post or tweets), his personal history and even his actions in real time. Each user, in the cybernetic ecosystem, has an autonomous life, interacts with other users of the net and defines its role in the digital society.

The aforementioned situation became possible by means of the numerous technologic functions provided by the Social networks: tools to publish images, videos and comments, instant messaging services (chat), localization through GPS (check-in), and the timetable concerning each virtual action realised by the user.

Therefore, if in each Social network the user owns a virtual identity, in the same manner, on the instrument remains trace of all the actions performed by him on the virtual platform supplied by the provider (3). Traces that, as concerns the languages used by the legislator, correspond to personal and sensible data, legally protected as containing information that could contribute to jeopardize the stability of the working relationship (4).

---

(2) Legal literature distinguishes between network, which mode of operation assumes that the user reveals its own identity both to other users and to the administrator in a vertical way (i.e. identifying) and network which does not require similar identification. The distinction is relevant for the logical structure of the program (which defines the manner in which the net can affect the users and the manner in which the users can interact between themselves), and seems to be also fundamental with reference to the application of the rules concerning data protection. In fact, only in relation to identifying networks the need to protect users' personal information is perceived.

(3) The Social networks are services provided by companies operating worldwide to allow people to virtually interact between themselves. According to Directive 98/34/EC, the suppliers are legally classified among the services provided by the information companies. In addition, whether the Social network, as usually happens, provides services of electronic communication, i.e. allows the user to publish contents created by himself (pictures, texts, music), also the rules set forth by Directive 2002/58/EC, referred to private life and electronic communications, are applicable.

(4) As to an analysis of the protections set forth by art. 8 St. lav. please see F. Iaquinta, A. Ingrao, *La privacy e i dati senbilii del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, *DRI*, 2014, 1027. Even if a detailed study of case law is not possible here, please consider the relevant case *Snyder v. Millersville Univ.*, No. 071660, 2008, U.S. Dist. LEXIS 97943, at 12-22 (E.D. Pa Dec. 3, 2008), concerning an elementary school teacher appeared drunk in a photo posted on My Space, who was dismissed since the employer considered her not appropriate to provide educational services.

Nevertheless, the problems related to the worker-user are wider. In fact, the abovementioned virtual life, full of solicitations and incitements, could move him to spend time to manage his image on Social networks, rather than to remain focused on the performance that he is bound to perform in reason of his employment agreement. The Social networks become, in this manner, a *divertissement* during the working time and on the working place. Socials also represent a dangerous distraction for preservation of job, in case the worker should interrupt his performance and leave the machineries, disobeying to the duty of care set forth by art. 2104 c.c., i.e. to chat with an handsome woman (5) or to challenge his friends playing with the apps downloaded on the device. In particular, Social networks are dangerous because the time not worked and spent on them consists in a diminution of productivity of one element of the company organization.

Social networks may allow the worker also to realize worse behaviour. As in the real life, the worker can perform illegal conducts (6). In addition, also an illegal conduct, in the technologic era, may be digitalized. The analysis of case law (7) highlights that, by means of an

(5) See the notorious case law Cass. 27th May 2015, n. 10955, *FI*, 2015, I, 2316, according to which the control from remote is legal, even if performed by means of the creation of a fake Facebook profile, in order to move the worker to chat, and this kind of control is aimed to ascertain a behaviour "harmful for the company assets, as to the regular activity and the safety of machineries".

(6) In particular, please consider the behaviour "which may cause damages to company assets, company machineries, and all company goods not relevant for working activity", see Cass. 3rd April 2012, n. 4746, *RGL*, 2002, 642 and *MGL*, 2002, 644, nt. Bertocchi; Cass. 17th July 2007, n. 15892, *RGL*, 2008, 358 and *RIDL*, 2008, 714, nt. Vallauri; Cass. 23rd February 2010, n. 4375, *RIDL*, 2010, II, 564; Cass. 23rd February 2012, n. 2722, *FI*, 2012, I, 1421; Cass. 1st October 2012, n. 16622, *FI,* 2012, I, 3328.

(7) The Relation of Italian Privacy Authority for the year 2010, p. 112, underlines the case of a worker dismissed in consequence of the use of Facebook: the employee published on his profile, accessible to "friends of friends", some pictures took in the company premises where, on the background, were portrayed also some technical projects covered, in the opinion of the company, by industrial secret. The abovementioned evidences have been declared valid and, consequently, the Court admitted the proposing party to use them, since the Facebook profile of the worker was, potentially, visible to an indeterminable group of users (the "friends of friends", indeed). It is interesting to consider, also, the case analysed by Trib. Milano, order, 1st August 2014, *RIDL*, 2104, commented by F. Iaquinta, A. Ingrao, *Il datore di lavoro e l'inganno di Facebook*; in particular, the worker, dismissed for cause, posted on his Facebook "public" profile some pictures, took during the working time, with characteristic of place and time demonstrating that the author left the working place during the working time and thus interrupted his performance. In connection with the aforementioned pictures, the worker posted also offensive comments as "how beautiful it is to work at the shitty A. Srl".

ordinary click, the company assets, considered from a wide point of view, and therefore comprehensive of intangible assets (i.e. the company's reputations among its clients, put at risk by means of workers' offences, the industrial secrets and the know-how revealed by pictures posted on Facebook), may suffer severe damages that could conduct the employer to retain "broken" the relationship of trust with a singular employee.

In reply to this broad list of illegal and defaulting behaviours (8), which represent also a breach of contract, that the employee may show on Social networks, the employer develops, always more frequently, the desire to know what the employee "does" on the digital platform. It is not only matter of curiosity to be satisfied, but sometimes the defensive reasons of the employer arise. This demand is sometimes satisfied through private investigations and surveillance aimed to discover these bad practices, and to obtain evidences to use in a judicial proceeding to avoid that these violations remain unpunished.

The technology provided by Web 2.0 is naturally a powerful partner of the controller. The abovementioned technical characteristics allow the employer to know from what place and during what time in the day the user is connected, to collect traces and evidences of the worker's fulfilment or not to his contractual obligations. One of the most relevant aspects of this technique, for employers, is that controls are free of charge and that Social networks are simple and accessible also for the old "*bonus diligens pater familias*". Notwithstanding, in addition, data and information registered by Social networks remain stored on the digital platform, also whether the user does not use his computer, smartphone or tablet provided him by the company. In fact, the control devices of Social network start independently of the proprieties of the instruments utilized by the user to accede to the platform.

The evolution of the Social networks, losing their original function of amusement and entertainment, urges one to reflect upon it. As to this point, the question to answer is whether the data that could be found on the Social network may be used as evidences in a judicial proceeding to sustain that a worker did not fulfil his contractual obligations or realized an illegal conduct. Moreover, in case of positive

(8) Since the beginning it seems important to underline the inseparable theoretical connection between illegal activity and defaulting behaviour to the obligation set forth by law as a consequence of the execution of an employment agreement, see P. Tullini, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, *RIDL*, 2011, II, 89. The Author underlines that, in the most part of case law, the interference between illegal activity and defaulting behaviour «exists and can not be removed».

answer to the previous question, the following issue is what are the limits set forth by the local legal framework.

To find an answer to the abovementioned questions it is necessary to analyse the evolution of the structure of rules on which is based the discipline of the controls from remote, after the reform concerning art. 4 St. lav.