CSP CADERNOS DE SAÚDE PÚBLICA
REPORTS IN PUBLIC HEALTH

ARTIGO
ARTICLE

Cyber dating abuse or proof of love? The use of apps for surveillance and control in affective-sexual relations

Abuso digital ou prova de amor? O uso de aplicativos de controle/monitoramento nos relacionamentos afetivo-sexuais

¿Maltrato digital o prueba de amor? El uso de aplicaciones de control/seguimiento en relaciones afectivo-sexuales

Roberta Matassoli Duran Flach [1,2]
Suely Ferreira Deslandes [1]

doi: 10.1590/0102-311X00060118

Abstract

Contemporary digital culture is marked by intermingling borders between the public and private spheres, urging internauts to be both controllers and controlled. The article analyzes the discursive productions on surveillance and control of partners by online tools provided by the Android and iOS systems, available as cellphone apps. The authors use critical discourse analysis to examine and interpret text messages from 40 Android and iOS apps used to monitor and control intimate partners. We identified two blocks with two distinct (but not mutually exclusive) discursive meanings: control/monitoring and care/protection. The texts' enunciative force is based on a promise of total and unlimited control with the purpose of ensuring "peace of mind", "safety/ security", and "harmony" in the intimate relationship. Such surveillance uses rhetorical arguments that refer to "proof of love", "care", and "protection" as justifications for monitoring and controlling the other.

Intimate Partner Violence; Mobile Apilications; Internet

Correspondence
R. M. D. Flach
Instituto Nacional de Saúde da Mulher, da Criança e do Adolescente Fernandes Figueira, Fundação Oswaldo Cruz.
Av. Rui Barbosa 716, 2o andar, Rio de Janeiro, RJ 22250-020, Brasil.
matassoli@gmail.com

[1] *Instituto Nacional de Saúde da Mulher, da Criança e do Adolescente Fernandes Figueira, Fundação Oswaldo Cruz, Rio de Janeiro, Brasil.*
[2] *Corpo de Bombeiros Militar do Estado do Rio de Janeiro, Rio de Janeiro, Brasil.*

Introduction

With the widespread use of Internet, social relations are now mediated by digital communication technologies at unprecedented levels, facilitating the creation of an associative and community linkage, or digital sociality [1,2]. This sociality is characterized by a set of daily practices and collective experiences based on a plurality of values, mediated by network architecture, exponentially expanding and contributing to a process known as retribalization of the world [1,2], i.e., groupings that happen via common interests, regardless of fixed borders or territorial demarcation.

In this sense, the virtual is the materialization of a continuous deterritorialization of the real, affecting the way we deal with time. The idea of future, space, time, and territory are modified by the introduction of microelectronics and telematic networks, producing the sensation of space-time compression through diverse forms of social aggregation [3].

Although such digital relations have their own dynamics, which are still poorly understood, they are not free of the same forms of power configuration based on gender, class, and ethnicity (important markers of social inequalities in the "off-line world").

Meanwhile, these new forms of social aggregation create and reproduce a new group ethos, i.e., a new way of being, of belonging, of existing in contemporary society in which there are no more borders or territorial boundaries (cyberculture or digital culture) [1].

Digital culture has empowered gregarious and retribalized drive [4], acting as a vector for communion and sharing of feelings and community reconnections of all ideological and ethical types, whether in the defense of rights and respect for otherness, or in segregation and violence. This process tends to impregnate society as a whole [1,5].

All these changes have only been possible thanks to network architecture, based on a technology that produces and mediates information, representations, and discourses that influence and are influenced by and converse with other media by which information circulates rapidly [1,6].

The ease with which these networks expand, reconfigure, change, and adapt without losing their basic characteristics and without leaving traces of their paths exponentially increases the possibility that the information generated in the process will quickly gain visibility [7].

The many elements that sustain digital culture feature overvaluing of public exposure or "hypervisibility", in which the borders between what had been considered public and private for decades now intermingle and dilute, turning the act of "snooping" into a fundamental part of digital sociality [5].

We are thus living in the "Age of Exhibitionism", i.e., submitted to a constant plea for collective "publicity", urged to spontaneously and voluntarily announce everything related our private lives, turning personal secrets into an open book of personal promotion. According to Recuero [8] (p. 135), this practice *"is seen as a sort of 'social capital' that builds such values as intimacy, trust, and proximity between the actors..."*.

There is thus a shuffling of boundaries between control and visibility, public and private, which feed back into each other and simultaneously constitute a "surveillance aesthetic" [9], urging everyone to be both controllers and controlled.

The Internet's popularity, especially with so-called web 3.0 (the advent of social networks), ushered in an Age in which interpersonal contacts are formed anywhere in real time, allowing an unprecedented form of protagonism, permitting and urging the continuous construction of self- representations and self-narratives in digital space [6].

There is no location or secret in the new Age of digital culture that cannot be discovered [9]. We live in pursuit of "the other's view", of acceptance and approval via "likes", the number of followers and shares in digital social networks *"continuously making our own fame for the world"* [5] (p. 32) as a sort of "narcissism epidemic" [10] or "simulated voyeurism" [9].

Private life is externalized in search of a view that acknowledges and attests to it visibility, a self-image in a world where our existence requires being seen and witnessed by millions of spectators [9] in a constant and intermittent process of "negotiating identities", or rather, constantly affirming one's own identity. Virtual communities have allowed individuals to interact, while also creating the possibility of forging their own characteristics [6], manipulating data pertaining to their identity [11], and living "multiple selves" [12].

However, the issue is not to polarize the debate between victims and aggressors, since it is precisely the contours of digital sociality, marked by exhibitionism affecting everyone indiscriminately, that encourages participants to break down the boundaries between public and private. Importantly, there is an intrinsic relationship between the technological architecture that defines the digital platforms on which social networks (a level of technical procedures taking place far from the users' more concrete experience) and these overexposure practices are performed. In fact, it is precisely this technological base that provides the conditions (while conditioning) digital sociality, constantly suggesting practices of sharing privacy.

Virtual communities such as Facebook, Instagram, Twitter, WhatsApp, and Messenger are symbolic spaces of sharing and belonging [1]. Through the digital social networks, this simulated voyeurism and "image overexposure" are easily exercised, establishing the basis for relationships that range from searching for new friendships to affective-sexual relations with various degrees of commitment.

The affective-sexual relations and expressions mediated by digital social networks also become fertile ground for the development of new practices of violence between partners, known as cyber dating abuse [13,14,15,16,17,18].

Cyber dating abuse includes humiliation, insults, threats, control, and isolation, largely similar to the characteristics of off-line abuse [13,14,15,16,17,18]. Still, cyber abuse has greater potential for propagation, given the nature of sharing and dissemination provided by the Internet.

Cyber dating abuse is typified in various ways, with non-consensual sexting, revenge porn, and control/monitoring as the main modalities.

Consensual sexting is not classified as a crime, and its practice is related to the dynamics and grammar of amorous-sexual seduction via sending sensual text messages, photos, and videos, with or without nudity, to a given person or group [19,20,21]. Still, non-consensual disclosure to third parties is a type of revenge porn and thus a form of cyber dating abuse [19]. Usually practiced at the end of an affective-sexual relationship as a form of retaliation, revenge porn is defined as posting intimate photos and videos without consent with the aim of degrading the former partner's image or taking revenge on him or her [22].

Due to the potential risk of the target's degradation and humiliation [17], cyber dating abuse is acknowledged by health professionals and its discursive practices as a type of psychological and emotional abuse. Such practices are identified by the literature as capable of harming the person's identity, self-esteem, integrity, privacy, and public image, leaving psychological scars [23,24].

The current article focuses on the practice of control/monitoring affective-sexual partners in various ways, tracking the last cellphone connection, using the personal password, checking the partner's emails and text messages without their authorization, creating fake profiles on social networks to monitor and control who the partner communicates with, and more recently, even installing tracking, controlling, and monitoring apps, usually without the person's knowledge.

The demand for control/monitoring has also become a commodity in this wide world of Internet business [5]. Tracking apps become popular and are frequently offered free of cost in the Android and iOS mobile phone systems and range from remote control of the partner's cellphone and the cellphone and email passwords, real-time location via GPS tracking, and even access to messages posted and received in social networks, WhatsApp, and SMS.

This study aims to analyze the discursive productions on cyber control and monitoring of partners. The locus of analysis is the apps offered by the Android and iOS systems.

Methodology

The study adopted critical discourse analysis (CDA), based on the assumption that language is a form of social practice [25]. In broad strokes we can say that social practices as a whole constitute a social order, with its bonds of influence and/or determination, and its semiotic aspect as an "order of discourse" [26]. An order of discourse is defined by Fairclough [26] (p. 310) as "*a particular social structuring of the relations between various ways of constructing meaning, that is, the various discourses and genres...*".

In its methodological perspective, for Fairclough [25], discourse analysis includes a three-dimensional conception that combines three analytical traditions, indispensable for discourse analysis: text analysis, discursive practices, and social practice.

Text analysis is based on categories such as vocabulary, grammar, cohesion, and text structure. In our study, the category "vocabulary" revealed the meanings of words and their metaphors, whether there were ambiguities and ambivalences, neologisms, or word switches. In "grammar", we observed the phrasing, the subject's position in the sentence (whether indeterminate, hidden, or present), and whether the sentences were worded in the active or passive voice. The category "cohesion" revealed the types of connections, nexuses, conclusions, deductions, and descriptions that were established, allowing the investigation of rhetorical schemes. In the "text structure" we analyzed the text's architecture, arguments, and contents.

In the discursive practice, we observed the dialectical relations between social structure and discourse and the way the texts are produced, interpreted, distributed, and consumed. The dimension of social practice refers to ideological and hegemonic effects such as knowledge and belief systems, constructions of social identities, and social reality [25]. In our study, this analysis was performed through a critical and crosscutting reading of ideological outputs in light of cyberculture's theoretical framework.

Our analytical corpus was based on a search in the paid or free Play Store (Android system) and App Store (iOS) that offered such services as intimate partner control, monitoring, and tracking. We used the following keywords: boyfriend tracker (RNo), girlfriend tracker (RNa), boyfriend spy (ENo), girlfriend spy (ENa), husband spy (EM), and wife spy (EE).

We initially identified 274 apps in the Android system and 201 in iOS. We then proceeded to a detailed reading of the material and excluded the following types of apps: spyware, music and karaoke, games, stories, books, meeting, messages on commemorative dates, poems, control of menstrual period, pregnancy, or diet, prank calls, on-line shopping, Internet memes, sundry tips and suggestions, apparent duplicates, apps that failed to specify the target public, apps for collective use by friends and family, and those that did not include affective-sexual partners in their opening description. We only included texts available in Portuguese, English, and Spanish, and several texts in Arabic were thus excluded.

After these procedures, the remaining material included 40 apps available in the Android system and one app in iOS. Since the only app identified in iOS is included in the apps located by Android, it was classified with the same number followed by the letter "a". The texts were analyzed according to the language in which they were made available by the app (20 in English and 20 in Portuguese). Texts in English were analyzed in their original, without translation. Our search did not locate any texts in Spanish.

In order to analyze the opening description on the app's main screen, the app's stated objective, the target public for control, identification of the developer, details pertaining to permission, the version, the charge for downloading the app onto the user's cellphone, the number of downloads, and the app's user ratings, we adopted the discourse analysis method, which we saw as a critical theory for dealing with the historical determination of processes of signification, aimed at problematizing established ways of thinking and explicitly revealing the ideological nature of speech [27].

Characterization of the material and the texts' architecture

Of the 40 apps, we identified only 33 developers, since some had created more than one app for the same purpose (App 5 through App 10, for example), with different names and sometimes for different target publics.

Some apps were rated by users from 1 to 5, and one is already in the 22nd revision. The number of downloads also varied greatly, from a hundred downloads to more than five million (Box 1).

In this new technological world, outstanding developers are those whose apps receive the best ratings and the most downloads among hundreds of thousands of competitors. Faced with increasingly well-informed users, the advertising world has been forced to create new approaches to address this increasingly demanding and actively participating audience [28]. "*It is for this new consumer* (...) *that advertisers are creating increasingly interactive strategies in order to gain their attention*" [28] (p. 34). Apps developers like the ones analyzed in the study thus adopt their own linguistic practices with the purpose of reaching the target public, with the aim of having their apps downloaded [29]. They generally foment a feeling of exclusion and of miss a fabulous opportunity in case one fails to purchase or acquire their app.

"This app was built to be quick, user-friendly, and without unnecessary features" (App 5, App 6).

"...it's the kind of app that's always handy to have in your cellphone. After all, you never know when you're going to need it" (App 7, App 8, App 9).

"Built for low energy consumption compared to similar apps..." (App 7, App 8, App 9).

"...user-friendly, simple, light, and functional without using unnecessary features (...) *low energy consumption* (...) *doesn't leave traces in the memory"* (App 8).

The targets for control by these apps are mostly affective-sexual partners (wife, husband, girlfriend, boyfriend, lover, "hookups"), followed by children, other relatives, and also employees, i.e., persons connected to relations in the sphere of intimacy and those in whom there is clear subordination, such as to the employer (Box 2).

We found that the apps' textual architecture follows a pattern, with one unstructured part (in which developers present their product) and another part preset by the operational system.

The structured text usually explains the "step by step" for the download, present in more than half of the apps in our sample (29). In some cases, the details for the download are accompanied by images that appear in the opening screen. They all display the app's name and logotype, the developer's name, and a publicity picture, followed by the unstructured textual production. Finally come the reviews, which are the user ratings and additional information, which show among other things the current version and the number of downloads (Box 1). The iOS system does not list the number of downloads.

In the unstructured text portion, developers provide a brief description of the app, with more complete information available through the offer of various "services", all suggesting that the app is better and more efficient than the others.

When the user shows interest in downloading the app, a screen pops up instantly called "permission details", authorizing the developer to control, from the mobile device, the location, photos/medias/files, contacts, telephone, call information and device code, identity, information on wi-fi connection, SMS, history of the device and apps, camera, and microphone. However, it does not explain to users what each of these permissions means in terms of access to the information stored in their cellphone.

Generally, in order to download a "free" app, various pieces of the users' personal information are solicited by the developer, who uses a resource called the "algorithm" to obtain private and intimate data, which are then used as currency with the companies. *"Algorithmization is defined as the set of suggestions provided by algorithms on sociality decisions and mechanisms for aggregation identified in the social networks' websites"* [30] (p. 1). *"Thus, through digital tracks left by the user, a developer is able not only to accumulate this information in a databank, but also to have these data contribute to analyses and cross-referencing of variables* (...) *as a way of steering* (…) *interest filters"* [30] (p. 2).

Such filters, by capturing the tracks left by users in the network and reaching conclusions on their interests, habits, and preferences, end up steering their attention to certain subjects and behaviors, [31] thereby mobilizing anther kind of market, based on the information emitted constantly by users of digital social networks. In other words, partner-control apps (like other apps) are also able to monitor and control the supposed controller.

"Peace of mind" ensured by "total control"

All the developers in this sample use verbs in the imperative and targeted to the audience with the aim of convincing the user of the product's efficiency. "Follow", "monitor", "track", "control", "prevent", "spy", and "be notified" are some of the main verbs used in the 40 apps, promising instrumental control efficacy (Box 2).

Many of the texts proclaim the promise of "peace of mind", "security", and "harmony" in the user's intimate relationship, resulting from the control/monitoring practices made possible by the apps. The promise is total and boundless control that can be exercised "anytime and anywhere", regardless of where the tracked person is or what they are doing, since the app informs everything that the monitored individual has done, without the user even having to leave the comfort of their home.

Box 1

Characterization of apps according to developer, anme of app, current version, free versus paid, user ratings, downloads, and serach key *.

App	Developer	Name of app	Current version	Free/ Paid	User ratings	Downloads	Search key
Android via Play Store							
1	Alexxfloo	Cellphone tracker	5.0 (updated 20/ Nov/2016)	Free	3.0	1,000-5,000	RNo, RNa, ENo, ENa, EM, EE
2	All Consult	RDC Cellphone tracker	5.0 (updated 30/ Oct/2014)	Free	4.2	100,000-500,000	RNo, RNa, ENo
3	AlPlugApps	Cell Phone Tracker	1.8.1 (updated 21/ Jul/2016)	Free	3.7	50,000-100,000	EM, EE
4	AnyTracking	Detective cellphone tracker	1.1.5 (updated 29/ Oct/2015)	Free	3.4	100,000-500,000	RNo, RNa, ENo, EM, EE
5	AppDroid Aplicativos Ponto Com	Boyfriend tracker	4.6 (updated 14/ Oct/2016)	Free	3.4	100,000-500,000	RNo, RNa, ENo
6	AppDroid Aplicativos Ponto Com	Girlfriend tracker	4.4 (updated 14/ Oct/2016)	Free	3.5	100,000-500,000	RNo, RNa, ENo
7	AppDroid Aplicativos Ponto Com	Track cellphone by number	1.9 (updated 12/ Dec/2016)	Free	3.5	100,000-500,000	RNo, RNa
8	AppDroid Aplicativos Ponto Com	“Where are You?” Tracker	2.2 (updated 04/ Oct/2016)	Free	3.3	50,000-100,000	RNo, RNa, ENo
9	AppDroid Aplicativos Ponto Com	Free Cellphone tracker	4.8 (updated 26/ Dec/2016)	Free	3.6	1,000,000-5,000,000	RNo, RNa, ENo
10	AppDroid Aplicativos Ponto Com	Pro Cellphone tracker	3.8 (updated 20/ Dec/2016)	Free	3.6	100,000-500,000	RNa
11	BytePioneers s.r.o.	Couple Tracker-Track Cellphone	1.69 (updated 11/ Jan/2017)	Free	4.1	1,000,000-5,000,000	RNo, RNa,
12	CS Systems Pvt Ltd.-iLocateMobile	Monitor any telephone	4.5.3 (updated 12/ Jan/2017)	Free	3.7	1,000,000-5,000,000	RNo, RNa, ENo, ENa, EM
13	Darsh	Locator	18 (updated 27/ Dec/2016)	Free	4.6	1,000-5,000	RNa
14	Davidsonmue Tomunen	GPS Cellphone location	1.0 (updated 25/ May/2016)	Free	3.6	10,000-50,000	RNa, ENa
15	DenDev	GPS Control (Free)	1.2 (updated 27/ May/2013)	Free	3.0	10,000-50,000	RNa, ENa
16	DevKir	Mobile SMS Tracker	3.1.1 (updated 26/ Mar/2015)	Free	3.3	50,000-100,000	EM
17	Free vpn location dev	Find Phone Location Advice	1.0 (updated 22/ Jan/2017)	Free	New (recent launch)	New (recent launch)	RNo, RNa, ENo
18	Fugasam	Telephone tracking	1.0 (updated 16/ Dec/2016)	Free	3.2	1,000-5,000	RNo, RNa, ENo, ENa, EM, EE
19	Geeks n Ninjas	Randoms: Mobile Tracker	1.0 (updated 18/ Jun/2014)	Free	3.5	1,000-5,000	RNo, RNa
20	Innohabit Technologies	Trust Me More	1.8 (updated 26/ Feb/2016)	Free	3.4	100-500	RNo, RNa, ENo
21	IT Soft Dynamics	People Location Finder	PLF6 (updated 19/ Nov/2015)	Free	4.0	10,000-50,000	RNo, RNa
22	Jade SA	Mobile Phone Tracker	22 (updated 6/ Dec/2016)	Free	3.4	5,000-10,000	EM, EE
23	Leeway Applab	Whatscan	1.0.1 (updated 16/ Jan/2017)	Free	4.0	500-1,000	ENo, ENa, EE

(continues)

Box 1 (continued)

App	Developer	Name of app	Current version	Free/ Paid	User ratings	Downloads	Search key
Android via Play Store							
24	MateXPlore	TrustMate App	1.0.1 (updated 14/Jan/2017)	Free	4.4	100-500	RNo, RNa, ENo
25	MaxLo	Mobile Phone Tracker	4.2.1 (updated 23/Mar/2015)	Free	3.8	10,000-50,000	RNo, RNa, ENo
26	Mcgill Dias	Coliseum Tracker	2.3 (updated 17/Nov/2016)	Free	4.2	1,000-5,000	RNo, RNa,
27	MNA Team	Couple Monitor Device Tracker	1.0.3 (updated 06/Dec/2016)	Free	3.7	10,000-50,000	RNo, RNa, ENo
28	Omega Solutions	Mary's Boyfriend Tracker	2.8 (updated 17/Aug/2016)	Free	3.0	100-500	RNo, RNa, ENo
29	Omega Solutions	Pokies Girlfriend Tracker	2.8 (updated 17/Aug/2016)	Free	5.0	100-500	RNa
30	Peerzada Solutions	Track Me	1.0.3 (updated 11/Feb/2015)	Free	4.6	100-500	RNo, RNa
31	Sahil Jain	Musafir Trip	1.2.4 (updated 04/Jul/2015)	Free	5.0	100-500	RNo, RNa, ENo
32	Shiek Apps	Friends Tracker	2.1 (updated 17/Aug/2016)	Free	3.9	500,000-1,000,000	RNo, ENo
33	SoftSquare InfoSoft	Amiga Cellphone Tracker	1.18 (updated 08/Jan/2017)	Free	3.8	100,000-500,000	RNo, RNa, ENo
34	TGF Company	Boyfriend tracker	1.0.2 (updated 15/Jun/2014)	Free	2.8	10,000-50,000	RNo, RNa
35	Trila.Droid	GPS Location Tracker	2.2.0b (updated 17/Feb/2016)	Free	4.0	500,000-1,000,000	RNo, RNa, ENo
36	Trila.Droid	GPS Location Tracker Pro	2.2.0b (updated 17/Feb/2016)	BRL 8.16	4.1	500-1,000	RNo, RNa, ENo
37	Windorado.com	Love Keeper – Cheater Alert	2.0.3 (updated 14/May/2014)	Free	2.6	10,000-50,000	RNo, RNa
38	Xevate	IpSpy monitor anywhere	Ipspy.1 (updated 25/Aug/2016)	Free	1.0	100-500	EM
39	ycventure	Tracker Cellphone	1.1 (updated 06/Aug/2016)	Free	3.4	10,000-50,000	RNo, RNa, ENo
40	Zaid Ahmed	Location Tracker	1.0 (updated 24/Mar/2014)	Free	3.6	1,000-5,000	RNa
iOS via App Store							
4a	Luciano M. A. Cardoso	AnyTracking	1.2.2 (uptdated 09/Apr/2016)	Free	> 4	-	RNo, RNa

EEE: wife spy; EM: husband spy; ENa: girlfriend spy; Eno: boyfriend spy; RNa: girlfriend tracker; RNo: boyfriend tracker.

* Search performed on 28/Jun/2017.

Box 2

Characterization of apps according to stated objetive and target public.

App	Objective *	Target public for control
1	Monitor, children, employees, and personal life	Children, wife, husband, girlfriend, boyfriend, lover
2	Follow mobile device's location remotely	Children, girlfriend, boyfriend
3	Track any mobile telephone	Wife, husband, employees
4	Monitor and track anyone in real time with their knowing	Children, husband, wife, boyfriend, girlfriend, employees
4a	Monitor and track whoever you want in real time	Children, husband, wife, employees, technicians, executives, representatives
5	Track boyfriend's location	Boyfriend, wife, hookup
6	Track girlfriend location	Girlfriend, wife, hookup
7	Track cellphone via sharing location in real time, using the phone number	Children, girlfriend, friends, family
8	Track cellphone via sharing location in real time, using the phone number	Friends, family, loved ones, boyfriends, children
9	Track cellphone via sharing location in real time, using the phone number	Friends, family, loved ones, boyfriends, children
10	Track cellphone via sharing location in real time, using the phone number	Friends, family, loved ones, boyfriends, children
11	Prevention and detection of cheating and extramarital affairs	Partners, lovers, husbands
12	Track cellphone via GPS	Children, boyfriends, fiancés
13	Track current location	Sister, girlfriend, children
14	Track current location via GPS and SMS	Children, parents, girlfriend
15	Track current location via GPS	Children and girlfriend
16	Control all your loved ones	Children, employees, partners, and relatives
17	Track boyfriend's exact location	Boyfriend
18	Track cellphone to keep children safe, employee productive, and prevent cheating	Children, employees, boyfriend, girlfriend, husband, wife, lover
19	Monitor smartphone in real time via any web navigator	Children, employees, spouse, girlfriend, boyfriend
20	Track partner's location	Boyfriend, girlfriend
21	Send loved ones' precise location in real time	Children, boyfriend, girlfriend
22	Track wife/husband's location via cellphone	Wife, husband
23	Clone another WhatsApp account to monitor chat messages, images, and videos	Children, wife, boyfriend, girlfriend
24	Monitor partner to reduce risk of cheating and jealousy	Girlfriend, boyfriend, wife, husband
25	Monitor cellphones	Children, elderly, and partner (girlfriend, boyfriend)
26	Track anyone's location	Children, employees, boyfriend, girlfriend, luggage
27	Monitor partner	Spouse, boyfriend, girlfriend, fiancé
28	Track location of boyfriend	Boyfriend
29	Track location of girlfriend	Girlfriend
30	Track partner and friends	Boyfriend and loved ones
31	Track location	Sin, daughter, girlfriend, boyfriend, wife
32	Track location	Friends, family, girlfriend, boyfriend
33	Locate girlfriend in real time via cellphone	Girlfriend, boyfriend
34	Track and monitor boyfriend remotely	Boyfriend
35	Track location via GPS	Boyfriend, girlfriend, children, elderly, friends, employees
36	Track location via GPS	Boyfriend, girlfriend, children, elderly, friends, employees
37	Track location of partner to monitor whether they are cheating on you	Partners
38	Monitor anything	Babies, husbands, wives
39	Track location via GPS	Friends, family, boyfriend, girlfriend
40	Track location of children and boyfriend	Children, boyfriend, girlfriend

* Identified through the reseracher's analysis.

"...monitor, track, enjoy peace of mind..." (App 4, App 4a).

"Enjoy the peace of mind you need. Download this app onto your cellphone, activate the tracker, and you're done!" (App 9).

"Stop having to worry" (App 15).

Developers extoll their products' advantages based on strong textual cohesion [25] that establishes links between practicality & security and speed & efficiency – important values in the relations established in cyberculture [1].

Other developers offer additional advantages associated with their apps that corroborate the notions of security and tranquility. In addition to promising to monitor loved ones, some apps also track the cellphone device itself in case of loss or theft, which proves strategic for the argument of relevance and usefulness, given the "essential" role played by the cellphone in daily life and in this digital age. We use this medium to connect to the world, schedule dates with friends, organize work meetings, conduct bank transactions, publicize aspects of our private lives in on-line social networks and... control our partners, all of this in split seconds and twenty-four/seven.

"You can also use this app as an anti-theft solution to track your phone in case it's stolen" (App 1).

Importantly, while constant surveillance finds a rhetorical justification in the "prevention of violence" [32], it also establishes other forms of violence, these of a symbolic nature, based on controlling the other. Thus, it should not seem odd if "total control" is seen as a solution, as "peace of mind" ensured by cyber tracking and the promise that nothing can escape the gaze of the person doing the monitoring.

"Deleting text messages and calls is useless (...). *It's impossible to hide activities or remove communications"* (App 11).

"Nobody can escape you now (...) *not even your boyfriend"* (App 12).

"Nothing can be hidden from this app" (App 27).

"You can love in peace for the rest of your life" (App 37).

"Monitor anything, anytime, anywhere" (App 38).

Cyber dating abuse or proof of love and care?

The analysis of the texts on the services provided by the apps identified two blocks with distinct discursive meanings: (1) control/monitoring and (2) care/protection. The apps sometimes adopt a single discursive line, while at other times they combine the two.

In the block on control/monitoring (present in 25 apps), there is an obvious intertextual practice in which the discourses refer to the discursive fields of public safety/security and health. The typical lexica in these fields appear constantly and sometimes interconnectedly: "track", "control the location", "spy", "have peace of mind"; and "prevent", "follow", "monitor", "detect", "reduce risks", reduce what are considered harmful behaviors.

"If you want to follow your wife/husband, just download our tracking app..." (App 3).

"Never lose sight of the one you love (...) *monitor, track, have peace of mind..."* (App 4).

"...the best mobile app to prevent and detect cheating and extramarital affairs by partners, lovers, and husbands!" (App 11).

"...helps uncover partners' cheating, reduces the risk of infidelity/extramarital affairs, and reduces your love's jealous behavior" (App 11).

"...it's used to clone another wp account in your cellphone to monitor chat messages, pictures, and videos" (App 23).

Some apps offer additional features, which are also announced as "essential and unbeatable", especially for whoever wants to control and monitor their partner, such as "Geo-fencing" and the "Arrived?" mode, which define the territory in which the partner usually circulates, allowing to track changes in their itinerary.

"Geo-fencing: you can set a limited location area for your girlfriend. If she leaves the area, you receive an alert" (App 33).

"...In Arrived? mode, you mark a location on the map and choose a cellphone to monitor. If the app detects that the monitored cellphone has arrived at that location, the user receives a beep alert" (App 10).

However, the metaphor that best illustrates the fencing relationship established by these apps is the module called "electronic fence", adopted by eight apps. The "Electronic Fence" or "Virtual Fence" has the same basic purpose as the previous modules. The metaphor suggests both the demarcation of boundaries on a property, determining who is inside or outside the limits set by the owner, and the idea of virtual incarceration, with circulation restricted to a defined perimeter.

"Electronic Fence: In the Electronic Fence mode, the app makes a virtual connection to the tagged cellphone and begins to monitor it to detect changes in position. If the program detects that the cellphone has moved outside the electronic fence, the user receives a beep alert" (App 7).

In the block on care/protection (found in 7 apps), the intertextual practice includes discourses in which surveillance is largely confused with lexica that invoke meanings from an ethic of care, under the justification that the person is watching over the loved ones' physical integrity.

"Know where your children are, whether they're safe" (App 2).

"Worried about your loved one's safety?" (App 5 and App 6).

"No need to worry about your son, daughter, boyfriend, or girlfriend, because (...) *you'll be following all of them!"* (App 31).

"Stop worrying about your child or a girlfriend that doesn't answer the phone. Just press the button and find out where they are!" (App 15).

One of the few apps that suggests that the partner should know and approve of being monitored (or in case of being caught in this non-consensual practice) "teaches" the user to rely on the rhetorical argument of "proof of love" for negotiating and convincing the partner [13,14,33].

"...ask your boyfriend if he loves you, and if he says 'yes', ask him to download (...) *this tracking app..."* (App 12).

Among the apps with discourses involving both control/monitoring and care/protection (8), some presented the objective of control exclusively for partners and protection/care for children and parents. Others stated both objectives indiscriminately.

"You can control your children and elderly and your partner's phone" (App 25).

"Protect your innocent loved one..." (App 37).

The discourse adopted for employees focuses on controlling their activities to keep them productive and monitor whether they are completing the tasks determined by the employer, drawing on a discourse that emphasizes similar practices to those developed in the panoptic model.

"Control your team..." (App 2).

"You can use it to keep your (...) *employee productive"* (App 18).

Legality versus illegality of non-consensual monitoring

Concerning the legality of downloading an app in order to spy on someone without their knowledge or consent, only two developers displayed any concern for informing the monitored person, sending constant alerts and even requesting written authorization from the tracked individual.

"...the cellphone's owner will always be aware that their phone is being monitored (...)*. You may need written permission from the phone's owner"* (App 1).

"...a persistent notification will be displayed on the cellphone, preventing this app from being used as a spouse tracker with a hidden app" (App 18).

Of the 38 remaining apps, 26 did not even mention the matter of illegality, and 12 adopted the discourse of legality but without creating mechanisms to guarantee it (six of these apps were by the same developer: App 5 through App 10).

"...assumes permission by the user who has it downloaded and activated in the device (...) *can only be downloaded and used in devices that belong to the user or where the person carrying the device is aware and agrees to being monitored"* (App 8).

"Remember that this is not a spy app (...) *the family or friends should be aware that a phone tracking service is being executed in their cellphone..."* (App 12).

"We want you to know that this is not a spy app! Spying is illegal and can lead to a number of problems" (App 22).

The increasingly widespread use of technological resources along with ease of Internet access and connectivity have contributed to greater exposure to the risk of activities in the on-line world that are considered capable of harming others. Such acts, when classified juridically, are called "cybercrimes". However, in the Brazilian case many abusive conducts are not classified legally, producing a collective feeling of impunity in the on-line world [34].

Brazil did not ratify the Budapest Convention on Cybercrime [35] in 2001, which has been signed by 43 countries, including France, Italy, Portugal, Spain, United States, Canada, Japan, South Africa, Australia, Chile, and Argentina. The Convention's articles include Article 6 on "Misuse of devices", which includes criminal offenses involving confidentiality, integrity, and availability of computer systems and computer data, among others, "illegal access" (Article 2) via infringing security measures with the intent of obtaining computer data or other dishonest intent; "illegal interception" (Article 3) of computer data by technical means; "data interference" (Article 4) with the intent of damaging, deleting, deteriorating, alterating, or suppressing computer data; and "system interference" (Article 5) or serious, intentional, and illegal hindering of a computer system's functioning [35].

In the interim, there were various debates in Brazil between organized civil society and Congress, culminating in the passage of *Law n. 12,965/2014*, or the "Internet Civil Framework" [36], which establishes principles, guarantees, rights, and duties pertaining to Internet use in Brazil, regulating the protection of privacy and use of personal data. The law is the first government initiative in the attempt to prevent excesses committed in the on-line medium and avoid new infringements, reducing the feeling of legal impunity. However, the law's enforcement is still insipient, and the legislation is not clear in the case of the apps analyzed here.

Thus, non-consensual monitoring via apps provided by the Android and iOS systems in Brazil is an ambiguous terrain: although it is still considered an "illegal act" by international legal standards, it still lacks a clear definition under Brazil's domestic legislation, thus slipping to a more flexible situation, subject to diverse interpretations, with the status (at most) of "morally reproachable" conduct.

Final remarks

This study aimed to highlight how growing Internet access has promoted new forms of on-line sociality, as well as the banalization of abusive practices through the use of these same on-line media, justified by rhetorical arguments acclaiming the "if you love, you care" perspective, controlling, monitoring, tracking, and spying.

Total control comes to be seen as a way of ensuring "peace of mind", by which one takes for granted the use of apps which, via remote control and without the partner's consent, one eliminates the right to freedom and the inviolability of personal information.

Such practices rooted in the daily reality of affective-sexual relationships reiterate old forms of violence. The unequal power relationship within the intimate relationship, associated with this need for "total control" of the partner, is linked to the gender perspective, known in the literature and in the current study under the "care and control" dichotomy. Still, we did not detect an explicitly sexist nature in the material, since the texts are addressed to both male and female controllers. No data are available on who uses such apps most often or how they are handled in distinct relational contexts. More studies are needed, analyzing how such apps function and how they are employed in the daily power negotiations of affective-sexual relationships. Neither do we know which levels of negotiations are established between the "controller" and the "controlled" in the use of these apps: whether entirely without knowledge or permission or even the opposite, having knowledge and giving permission as a form of submission or as a strategy to make the partner believe that he or she actually exerts such control.

Likewise, the illegality of non-consensual monitoring is treated ambiguously by the apps, attempting to exempt developers from any legal liability.

Given the nature of this new digital sociality in which we are coaxed into overexposure and to become both controllers and controlled, the extensive reciprocity of such cyber dating abuse suggests the need for more in-depth and extensive studies aimed at understanding how these dynamics interact, producing and reproducing well-known violent practices, now further enabled in the new space of social interaction known as the Internet.

Contributors

R. M. D. Flach and S. F. Deslandes contributed equally to the article's production.

Additional informations

ORCID: Roberta Matassoli Duran Flach (0000-0002-1260-216X); Suely Ferreira Deslandes (0000-0002-7062-3604).

References

1. Lemos A. Cibercultura: tecnologia e vida social na cultura contemporânea. 7ª Ed. Porto Alegre: Editora Sulina; 2015.
2. Maffesoli M. Transfiguração do político: a tribalização do mundo. Porto Alegre: Editora Sulina; 2011.
3. Lévy P. Cibercultura. São Paulo: Editora 34; 2010.
4. Maffesoli M. O tempo das tribos: o declínio do individualismo nas sociedades de massa. Rio de Janeiro: Editora Forense Universitária; 2014.
5. Keen A. Vertigem digital: por que as redes sociais estão nos dividindo, diminuindo e desorientando? Rio de Janeiro: Editora Zahar; 2012.
6. Lima AS. Da cultura da mídia à cibercultura: as representações do eu nas tramas do ciberespaço. In: III Encontro de Pesquisa em Comunicação e Cidadania. Goiânia: Faculdade de Informação e Comunicação, Universidade Federal de Goiás; 2009. https://mestrado.fic.ufg.br/up/76/o/ciberespaco_representacoes_do_eu.pdf (accessed on 02/Nov/2017).
7. Martino LMS. Teoria das mídias digitais: linguagem, ambientes e redes. 2ª Ed. Petrópolis: Editora Vozes; 2015.
8. Recuero R. A conversação em rede: comunicação mediada pelo computador e redes sociais na internet. Porto Alegre: Editora Sulina; 2014.
9. Bruno F. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Ciber Cultura. Porto Alegre: Editora Sulina; 2013.
10. Twenge J, Campbell WK. The narcissism epidemic: living in the age of entitlement. New York: Free Press; 2009.
11. Rosa GAM, Santos BR. Repercussões das Redes Sociais na Subjetividade de usuários: uma revisão crítica da literatura. Temas Psicol (Online) 2015; 23:913-27.
12. Rüdiger F. Elementos para a crítica da cibercultura: sujeito, objeto e interação na era das novas tecnologias de comunicação. São Paulo: Hacker Editores; 2002.
13. Borrajo E, Gámez-Guadix M, Pereda N, Calvete E. The development and validation of the cyber dating abuse questionnaire among young couples. Comput Human Behav 2015; 48:358-65.
14. Borrajo E, Gámez-Guadix M, Calvete E. Justification beliefs of violence, myths about love and cyber dating abuse. Psicothema (Oviedo) 2015; 27:327-33.

15. Yahner J, Dank M, Zweig JM, Lachman P. The co-occurrence of physical and cyber dating violence and bullying among teens. J Interpers Violence 2015; 30:1079-89.
16. Dick RN, McCauley HL, Jones KA, Tancredi DJ, Goldstein S, Blackburn S, et al. Cyber dating abuse among teens using school-based health centers. Pediatrics 2014; 134:e1560-7.
17. Zweig JM, Lachman P, Yahner J, Dank M. Correlates of cyber dating abuse among teens. J Youth Adolesc 2014; 43:1306-21.
18. Zweig JM, Dank M, Yahner J, Lachman P. The rate of cyber dating abuse among teens and how it relates to other forms of teen dating violence. J Youth Adolesc 2013; 42:1063-77.
19. Flach RMD, Deslandes SF. Abuso digital nos relacionamentos afetivo-sexuais: uma análise bibliográfica. Cad Saúde Pública 2017; 33:e00138516.
20. Barros SC, Ribeiro PRC, Quadrado RP. Sexting: entendendo sua condição de emergência. EXEDRA Revista Científica ESEC 2014; 2014 Suppl:192-2013.
21. Ventura MCAA. Violência no namoro: crenças e autoconceito nas relações sociais de gênero. Modelo de intervenção em enfermagem [Tese de Doutorado]. Porto: Universidade de Porto; 2014.
22. Martsolf D, Colbert C, Draucker C. Adolescent dating violence prevention and intervention in a community setting: perspectives of young adults and professionals. Qual Rep 2012; 99:1-23.
23. Martinez C. An argument for States to outlaw "revenge porn" and for Congress to Amend 47 U.S.C § 230: how our current laws do little to protect victims. Journal of Technology Law & Policy 2014; 14:236-52.
24. Tungate A. Bare necessities: the argument for a "revenge porn" exception in Section 230 immunity. Information & Communications Technology Law 2014; 13:172-88.
25. Fairclough N. Discurso e mudança social. Brasília: Editora UnB; 2001.
26. Fairclough N. Análise crítica do discurso como método em pesquisa social científica. Linha D'Água 2012; 25:307-29.
27. Minayo MCS. O desafio do conhecimento. Pesquisa qualitativa em saúde. 12ª Ed. São Paulo: Editora Hucitec; 2010.
28. Barichello EMMR, Oliveira CC. O marketing viral como estratégia publicitária nas novas ambiências midiáticas. Em Questão 2010; 16:29-44.
29. Brei VA, Rossi CAV, Evrard Y. As necessidades e os desejos na formação discursiva do marketing – base consistente ou retórica legitimadora? Cadernos EBAPE.BR 2007; 5:1-21.
30. Moura CS, Gomes SHA. Com quem andas e com quem andarás: rastros digitais na algoritimização das relações. In: Anais do IX Simpósio Nacional da ABCiber. São Paulo: ABCiber; 2016. p. 1-16.
31. Parasier E. O filtro invisível: o que a internet está escondendo de você. Rio de Janeiro: Editora Zahar; 2012.
32. Bauman Z. Vida em fragmentos: sobre ética pós-moderna. Rio de Janeiro: Editora Zahar; 2011.
33. Borrajo E, Gámez-Guadix M, Calvete E. Cyber dating abuse: prevalence, context, and relationship with offline dating aggression. Psychol Rep 2015; 116:565-85.
34. Barreto ET. Crimes cibernéticos sob a égide da Lei 12.737/2012. Conteúdo Jurídico 2017; 07 mar. http://conteudojuridico.com.br/artigo.crimes-ciberneticos-sob-a-egide-da-lei-127372012.588644.html (accessed on 02/Nov/2017).
35. Council of Europe. Convention on cybercrime. Budapest: Council of Europe; 2001. (European Treaty Series, 185).
36. Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União 2014; 24 abr.

Resumo

Na cultura digital, há um embaralhamento entre as fronteiras do público e do privado, e nos convida a sermos, ao mesmo tempo, controladores e controlados. Este artigo analisou as produções discursivas sobre controle e monitoramento do parceiro veiculadas nas ferramentas digitais ofertadas pelos sistemas Android e iOS, disponíveis nos aplicativos de telefonia móvel. Adotamos a análise do discurso crítico para o exame e interpretação das enunciações textuais de quarenta aplicativos dos sistemas Android e iOS destinados ao controle de parceiros. Identificamos dois blocos com distintos sentidos discursivos não excludentes: controle/monitoramento e cuidado/proteção. A força enunciativa dos textos tem como base uma promessa de controle total e irrestrito com o propósito de assegurar a "paz de espírito", "segurança" e "harmonia" no relacionamento íntimo. Invocando para tal, argumentos retóricos que remetem à "prova de amor", "cuidado" e "proteção" como justificativas para o controle/monitoramento do outro.

Violência por Parceiro Íntimo; Aplicativos Móveis; Internet

Resumen

En la cultura digital, existe un terreno difuso entre las fronteras de lo público y privado que nos invita a ser, al mismo tiempo, controladores y controlados. Este artículo analizó los productos discursivos sobre control y seguimiento de la pareja, mediante herramientas digitales ofrecidas por los sistemas Android e iOS, disponibles en aplicaciones de telefonía móvil. Adoptamos el análisis del discurso crítico para el examen e interpretación de enunciados textuales de 40 aplicaciones con sistemas Android e iOS, destinados al control de parejas. Identificamos dos bloques con distintos sentidos discursivos no excluyentes: control/seguimiento y cuidado/protección. La fuerza enunciativa de los textos tiene como base una promesa de control total y sin restricciones, con el propósito de asegurar la "paz de espíritu", "seguridad" y "harmonía" en la relación íntima. Invocando para ello, argumentos retóricos que remiten a: "prueba de amor", "cuidado" y "protección", como justificativas para el control/seguimiento del prójimo.

Violencia de Pareja; Aplicaciones Móviles; Internet

Submitted on 24/Mar/2018
Final version resubmitted on 24/May/2018
Approved on 03/Aug/2018