“Is recruitment well protected against Behavioural Differences between Real and Virtual?”

Nadine Touzeau
Profiler, net-profiler, researcher in behavior of cybercriminals

Abstract: While we are talking about better securing our environment in real and virtual space, recruiters are increasingly looking for solutions and innovations to better know candidates responding to job offers. Artificial Intelligence, social network analysis, psychological tests are all used to reassure oneself more than to ensure the recruitment of a candidate. But are these supports reliable? Knowing that recruitment is increasingly on social networks, the virtual helping to change its behaviour with regard to my research work on Behavioural Differentiations between the Real and the Virtual and my theories as “Avatarization”, “Virtual Intelligences”, “Transverse Zone” developed in my scientific publications (Touzeau, 2017-18, 1) and books (Touzeau, 2015 / 2018, 2). Can recruitment be reliable as it is today in the face of behaviour developed in the virtual world? Can recruiting in a virtual environment allow itself to use the same techniques as in the real world?

Keywords: recruitment - Transverse zone – cybersecurity – virtual space - Behavioral differentiation – Avatarization – Virtual Intelligence - economic environment

Introduction:
Recruitment is a strategic entry point into the company that cannot be underestimated and must be taken seriously. This profession integrates the human being.

Robert Half (3), 52% of human resources managers give as much or more importance to soft skills than to hard skills! He adds that to reinforce his choice of candidate, it is preferable to ensure this choice by personality tests that will reveal eight personality traits, 6 personal values and 3 revealing behaviours for a good knowledge of the candidate.

Recruitment is not therefore a step to be underestimated, especially since virtual space has invaded our environment.

In addition to the fact that the virtual space must be perfectly understood and integrated into our professional and personal lives, it cannot be subtracted or even neglected when searching for and selecting candidates, whatever the sector of activity. Luxury companies, defence structures, multinationals with entities located almost all over the world, small companies, associations, sensitive universes through the media coverage of products and/or people, must protect and protect their environment.

Are employees, in partnership, hired or subcontracted, sufficiently decoded to protect themselves from the risks of infiltration, fraud, cyber attacks, delinquency, etc.?

Considering the Behavioural Differences between the Real and the Virtual (Touzeau, 2015, 2018), do recruiters integrate these risks into their specifications?

Discussion
Meyer et al. (2001, 4) pointed out in particular that the validity of psychological tests is indeed very strong and quite comparable to the validity of medical tests (X-rays, magnetic resonance imaging and others) and that they make it possible to correct information allowing psychologists to better understand the problems submitted to them. It would be deplorable if psychologists, trainers, supervisors or educational institutions neglected or neglected what has historically been at the heart of psychologists' practice and earned them a certain, if not envied, notoriety.

However, there are many dysfunctions in the use of these tests. As written in this specialized journal on Business (Small Business, 4): "While some business leaders consider them essential, it is safe to say today that recruitment tests - whether personality tests or skills assessment tests, or both (so-called "psychotechnical tests") - are only recruitment tests..."
techniques, i.e. tools that the recruiter uses to minimize the risk of error."

Tests no longer seem to be a means of reassuring or informing recruiters about certain traits of candidates' characters. The lack of time, the risk of recruitment errors, the notion of results to avoid turnover, a form of recruitment security encourage the use of psychobiological tests, knowledge, personality sometimes even to the point of having the flows on social networks analysed by candidates. Reassure yourself and consolidate your results by taking as much support and care as possible in order to secure recruitment.

A recruitment error sometimes has serious consequences. In addition to wasting time, it is also a potential loss of information, with repercussions on colleagues, customers and partners. It can also lead to a loss of business, contracts. And finally, the notion of rumour that can be provoked following a disagreement, a disappointment.

In real space, impacts are relatively detectable and controllable. For an already obvious reason, which is diffusion. Indeed, the control of data leakage, contracts, information, research and even money can be better managed in reality without being able to contain, stop or recover it. It is easier in reality to reach malicious people without necessarily succeeding than in the virtual world.

The candidate is more and more inclined to make known on social networks his moods, his state of mind, his opinion, even his experience of the situation he is experiencing. A badly experienced recruitment can create a buzz on the internet (Olivia, 2019, 5) and give a very negative image of the company.

The candidate is more and more inclined to make known on social networks his moods, his state of mind, his opinion, even his experience of the situation he is experiencing. A badly experienced recruitment can create a buzz on the internet (5) and give a very negative image of the company.

The game changes when you consider that you broadcast on social networks what can perfectly be said in your living room in front of your family, without leaving it. Culturally, that's how we treated our setbacks. The unspoken was very common. Shameful part, to avoid making waves, out of respect, out of education. This is how grievances were handled.

The Internet has offered the potential to free itself by hiding behind the screen. It's like writing to your diary, or talk to yourself, or talk to your confidant, or speak out loud. Except that it is done on the web, in one click and it stays.

Two candidates with similar selection criteria, having the same type of job interview, will not react in the same way to the recruiter. They will interpret the statements made during the interview differently. It is even likely that few candidates would dare to do a tweet to express their feelings and comment on their job interview, until it creates a global buzz.

Behaviour that the Internet allows. One of the behaviors that my "Avatarization" (Touzeau, 2015) theory revealed. "Behind the screen, I express myself more easily than in real life and I allow myself to delve into things without thinking about the implications and without taking a step back and without discussing with the person with whom I disagree, or even misinterpreting what I say".... Reasons justified or not to disclose on the web its moods the incidences between the real and the virtual are notoriously different.

Then ensure discussions related to tweet, post, messages, especially if they are in the dissatisfied candidate's direction, will feed his feelings or that we are (Zone Transverse, Touzeau, 2015). Nevertheless, although the company replies, the candidate will be more likely to be credible to the detriment of the employer in the face of the multiple situations already experienced before by other candidates, but publicly silent. But also because it is ingrained in many mentalities, in France in any case, that the employer is not favoured whatever he does.

The sensitivity of recruiting from the Internet must consider these new behaviours that are discovered, developed and disseminated because of the virtual space. Any discussion cannot be considered confidential and closed because of a physical interview with few people in a confined space. Another subject mentioned was the assurance that the candidate was not an infiltrator, a kind of modern-day spy who would clone himself in order to integrate your company.

How many companies have their data stolen. Whether it is related to the customer file, research, accounting, internal culture, etc., company data is not only stolen in the virtual world. Competition is one of the significant players that promotes infiltration through recruitment. It's often easier to do industrial espionage. Thus, candidates will be able to easily find on the web the information they need to be recruited within the chosen company. Analysing the flow of employees in the company, the website, the organised activities are already enough to know how to get recruited.
This encourages cooptation, which is much appreciated by recruiters because it makes the task easier and saves time. Getting closer to the right people is often done by analyzing flows on social networks and physically meeting people. Playing the role that future employers expect will be easy for its malicious profiles. In fact, they will use controlled behaviour on the web, and also in front of people to seduce to be recruited. In fact, they will have enough information to know the recruitment steps and prepare for them. The processes being relatively widespread and generic, it is quite accessible to all. Thus, the reliability of the candidate allows the doubt that the information on the web is accessible by reading documents, comments, recruitment charter and making contact with the selected employees in order to be better integrated into the company. These infiltrations into companies can have serious consequences, such as the case of the former General Manager of LastMinute.com in France. Pierre Paperon (6) who found himself two years after the September 11 attacks in New York with an Al Qaeda member. He was hijacking airline tickets for his "friends". However, the recruitment was carried out according to the company's specifications and with tests. The target of a Tour Operator is interesting for infiltrators, especially terrorists. Any company has an interest for anyone who wants to be malicious with it. The hunting ground has increased due to the transversal nature of the Internet, which allows people to create false identities. Thus, fake PhDs, fake Curricula Vitae, fake LinkedIn sheets, fake recommendations that are mostly considered real by recruiters, are circulating on the Internet. If specialized structures are launched on the market in order to have a candidate's background checked, how many are fooled into recruiting profiles that are not what they claim. If this existed without the Internet, it is possible that the Internet could have encouraged the development of these false profiles in order to respond to real job offers in order to satisfy a real desire to exercise a profession that is considered one's own. Wouldn't recruitment by a dedicated diploma have also favoured this need to distort one's professional and educational career? Knowhow and interpersonal skills are often discarded by recruiters in favour of diplomas? Moreover, many countries no longer recruit on a diploma basis in the face of false diplomas that circulate too much and that are not always easy to verify. Finally, an end to a poorly considered and negotiated partnership can perfectly lead to a cyber attack. Ransonware is often the result of revenge following a conflict between employer and employee. Unsecured recruitment also at this location to avoid attacks paralyzing the company and its operations with data loss. Recruitment can be thwarted in several ways by the potential that the Internet offers to achieve its objective for a company. Security and cybersecurity do not seem to be major issues for companies. An essential question for recruiters is therefore to conduct recruitment differently in order to secure it and protect the economic environment: how to do it?

**Conclusion**

Realizing that recruitment is the secure entry point to a company is not really integrated by recruiters and business leaders. On the other hand, malicious people have understood it well and know how to use it. They play it and know how to use what they think is necessary to bring it to an end. Whether on behalf of a competitor, for personal revenge, in the name of an ideology or for oneself. The Internet tool is only a facilitator to obtain information, and play the role necessary to achieve its objective. Be the ideal candidate by using the necessary subterfuge. Meet the expectations that the company's culture requires by respecting the codes collected as contacts and readings related to the company progress. Create one or more characters and play their roles in the virtual and sometimes in the real world in order to obtain the desired position. So many possibilities are available to these candidates because of the Internet and the behaviour of recruiters who do not integrate these new behaviours that differentiate between the real and the virtual. They multiply tenfold, multiply it, develop thanks to and because of the Internet. Malicious people know how to do it. It is one of their weapons, one of their assets to play with the vulnerability of companies operating with the virtual as in the real world. The corporate culture displayed, the corporate values conveyed, the events, success stories, the very ego of the company published on the Internet, are all possibilities for malicious candidates who do not hesitate to use them. Everyone can use this information against the company. This is already the case for cybercriminals. Why not the candidates?

**References**

15.6 – Pierre Paperon - With a dual curriculum: scientific, ENSAM (Arts and Crafts) and management, MBA (HEC-ISA), Pierre PAPERON is now recognized as one of the best experts in the Blockchain. In this field, he has carried out missions in the energy sectors with TOTAL, VEOLIA, DALKIA, collaborated on cutting-edge international projects, worked in partnership with Microsoft and launched the observatoryblockchains.com:  https://medium.com/ @Pierre_Paperon/alqaida-dans-votre-entre pri se-que-faites-vous-82a7cd14b3ed