FUNDAÇÃO GETULIO VARGAS

DIREITO RIO

DIREITO E TECNOLOGIA

AUTOR: IVAR A. HARTMANN

GRADUAÇÃO
2014.1

Sumário

Direito e Tecnologia

OBJETIVOS

Capacitar os alunos para a tarefa de compreender os aspectos juridicamente relevantes de tecnologias da informação no séc. XXI.

Mapear as controvérsias de impacto social e compreender as respostas dadas pela jurisprudência aos problemas concretos, identificando congruências e incongruências da interpretação judicial quando estão envolvidas novas tecnologias da informação.

Auxiliar os alunos a pensar matrizes jurídicas para o enfrentamento dos atuais e dos futuros problemas a partir de uma compreensão adequada dos aspectos tecnológicos envolvidos nas controvérsias.

METODOLOGIA

Aula expositivo-dialogada, centrada principalmente em decisões judiciais ou administrativas, com leitura prévia e condução pelo método socrático.

Alguns dos temas são abordados mediante apresentação do problema e respectiva solução dada pela jurisprudência, com desenvolvimento de análise crítica sobre ambos. Outros temas são enfrentados como problemas em aberto, questões relevantes da vida e atividade comercial na sociedade-rede, que clamam ainda por soluções inovadoras e pensadas a partir de compreensões atuais de tais fenômenos e de respostas diferenciadas por parte do direito.

Os textos compilados no material didático são todos de acesso gratuito online. Trata-se quase sempre de recortes do livro, artigo ou decisão judicial, criteriosamente selecionados de modo a permitir ao aluno uma compreensão adequada ainda que com a leitura de uma porção pequena do todo ao qual se faz referência.

Nesse contexto, a leitura prévia dos textos indicados ou contidos nesse material didático são condição necessária, mas certamente não suficiente para cursar a disciplina. Os debates em sala de aula serão o centro da experiência. Ainda que a leitura prévia seja essencial, o protagonismo fica com o questionamento e construção coletivos.

A avaliação se dará com base na participação em aula e em na performance em prova inteiramente dissertativa e com consulta a todo e qualquer material a ser aplicada no final do curso.

CAPÍTULO 1 — DIREITO, TECNOLOGIA E CÓDIGO

Lawrence Lessig
Code 2.0

Chapter Two
four puzzles from cyberspace

EVERYONE WHO IS READING THIS BOOK HAS USED THE INTERNET. SOME HAVE BEEN in "cyberspace." The Internet is that medium through which your e-mail is delivered and web pages get published. It's what you use to order books on Amazon or to check the times for local movies at Fandango. Google is on the Internet, as areMicrosoft "help pages." But "cyberspace" is something more. Though built on top of the Internet, cyberspace is a richer experience. Cyberspace is something you get pulled"into," perhaps by the intimacy of instant message chat or the intricacy of "massively multiple online games" ("MMOGs" for short, or if the game is a role-playing game, then"MMORPGs"). Some in cyberspace believe they're in a community; some confuse their lives with their cyberspace existence. Of course, no sharp line divides cyberspace fromthe Internet.But there is an important difference in experience between the two. Those who see the Internet simply as a kind of Yellow — Pages-on-steroids won't recognize what citizens of cyberspace speak of. For them, "cyberspace" is simply obscure. Some of this difference is generational. For most of us over the age of 40, there is no "cyberspace," even if there is an Internet. Most of us don't live a life online that would qualify as a life in"cyberspace."But for our kids, cyberspace is increasingly their second life. There are millions who spend hundreds of hours a month in the alternative worlds of cyberspace — later on we will focus on one of these worlds, a game called "Second Life."1 And thus while you may think to yourself, this alien space is nothing I need worry about because it's nowhere I'll ever be, if you care to understand anything about the world the next generation will inhabit, you should spend some time understanding "cyberspace." That is the aim of two of the stories that follow. These two describe cyberspace. The other two describe aspects of the Internet more generally. My aim through these four very different stories is to orient by sometimes disorienting. My hope is that you'll come to understand four themes that will recur throughout this book. At the end of this chapter, I come clean about the themes and provide amap. For now, just focus on the stories.

BORDERS

It was a very ordinary dispute, this argument between Martha Jones and her neighbors.2 It was the sort of dispute that people have had since the start

of neighborhoods. It didn't begin in anger. It began with a misunderstanding. In this world, misunderstandings like this are far too common. Martha thought about that as she wondered whether she should stay; there were other places she could go. Leaving wouldmean abandoning what she had built, but frustrations like thiswere beginning to get to her. Maybe, she thought, itwas time tomove on. The argumentwas about borders — aboutwhere her land stopped. It seemed like a simple idea, one you would have thought the powers-that-be would have worked outmany years before. But here they were, her neighbor Dank and she, still fighting about borders. Or rather, about something fuzzy at the borders — about something of Martha's that spilled over into the land of others. This was the fight, and it all related to whatMartha did. Martha grew flowers. Not just any flowers, but flowers with an odd sort of power. They were beautiful flowers, and their scent entranced. But, however beautiful, these flowers were also poisonous. This was Martha's weird idea: to make flowers of extraordinary beauty which, if touched, would kill. Strange no doubt, but no one said thatMartha wasn't strange. She was unusual, as was this neighborhood. But sadly, disputes like this were not. The start of the argumentwas predictable enough. Martha's neighbor,Dank, had a dog. Dank's dog died. The dog died because it had eaten a petal fromone of Martha's flowers. A beautiful petal, and now a dead dog. Dank had his own ideas about these flowers, and about this neighbor, and he expressed those ideas — perhaps with a bit toomuch anger, or perhaps with anger appropriate to the situation. "There is no reason to grow deadly flowers," Dank yelled across the fence. "There's no reason to get so upset about a fewdead dogs,"Martha replied."A dog can always be replaced. And anyway,why have a dog that sufferswhen dying?Get yourself a pain-free-death dog, andmy petals will cause no harm." I came into the argument at about this time. Iwaswalking by, in theway one walks in this space. (At first I had teleported to get near, but we needn't complicate the story with jargon. Let's just say I was walking.) I saw the two neighbors becoming increasingly angry with each other. I had heard about the disputed flowers — about how their petals carried poison. It seemed tome a simple problemto solve, but I guess it's simple only if you understand how problems like this are created. Dank andMartha were angry because in a sense they were stuck. Both had built a life in the neighborhood; they had invested many hours there. But both were coming to understand its limits. This is a common condition:We all build our lives in places with limits. We are all disappointed at times. What was different about Dank andMartha? One differencewas the nature of the space, or context,where their argument was happening. This was not "real space" but virtual space. It was part of what I call "cyberspace." The environment was a "massively multiple online game" ("MMOG"), andMMOG space is quite different fromthe space we call real. Real space is the place where you are right now: your office,

your den,maybe by a pool. It's aworld defined by both laws that areman--made and others that are not. "Limited liability" for corporations is a man--made law. It means that the directors of a corporation (usually) cannot be held personally liable for the sins of the company. Limited life for humans is not aman-made law: That we all will die is not the result of a decision that Congressmade. In real space, our lives are subject to both sorts of law, though in principle we could change one sort. But there are other sorts of laws in real space as well. You bought this book, I trust, or you borrowed it fromsomeone who did. If you stole it, you are a thief, whether you are caught or not. Our language is a norm; norms are collectively determined. As our norms have been determined, your "stealing"makes you a thief, and not just because you took it. There are plenty of ways to take something but not be thought of as a thief. If you came across a dollar blowing in the wind, taking themoney will notmake you a thief; indeed, not taking themoneymakes you a chump. But stealing this book fromthe bookstore (even when there are so many left for others) marks you as a thief. Social norms make it so, and we live life subject to these norms. Some of these norms can be changed collectively, if not individually. I can choose to burn my draft card, but I cannot choose whether doing so will make me a hero or a traitor. I can refuse an invitation to lunch, but I cannot choose whether doing so willmakeme rude. I have choices in real life, but escaping the consequences of the choices Imake is not one of them. Norms in this sense constrain us in ways that are so familiar as to be all but invisible. MMOGspace is different. It is, first of all, a virtual space — like a cartoon on a television screen, sometimes rendered to look three--dimensional. But unlike a cartoon,MMOGspace enables you to control the characters on the screen in real time. At least, you control your character — one among many characters controlled bymany others in this space. One builds the world one will inhabit here. As a child, you grew up learning the physics that governed the world of Road Runner andWile E. Coyote (violent but forgiving); your children will grow up making the world of Road Runner andWile E. Coyote (still violent, but maybe not so forgiving). They will define the space and then live out the story. Their choices willmake the laws of that space real. This is not to say that MMOG space is unreal. There is real life in MMOG space, constituted by how people interact. The "space" describes where people interact — much as they interact in real space no doubt, butwith some important differences. InMMOG space the interaction is in a virtualmedium. This interaction is "in" cyberspace. In 1990s terms, people "jack" into these virtual spaces, and they do things there. And "they" turns out to be many many people. As Edward Castronova estimates,"an absoluteminimumfigurewould be 10million [butmy] guess is that it is perhaps 20 to 30million"participating in these virtual worlds.3 The "[t]ypical user spends 20 — 30 hours per week inside the fantasy. Power users spend every availa-

blemoment."4 As one essay estimates,"assuming just average contact time among these 9.4million people, subscribers to virtual worlds could be devoting over 213million hours per week to build their virtual lives."5 The things people do there are highly varied. Some play role-playing games: working within a guild of other players to advance in status and power to some ultimate end. Some simply get together and gab: They appear (in a form they select,with qualities they choose and biographies they have written) in a virtual roomand typemessages to each other. Or they walk around (again, the ambiguity is not a slight one) and talk to people. My friend Rick does this as a cat — a male cat, he insists. As a male cat, Rick parades around this space and talks to anyone who's interested. He aims to flush out the cat-loving sorts. The rest, he reports, he punishes. Others domuchmore than gab. Some, for example, homestead. Depending on the world and its laws, citizens are given or buy plots of undeveloped land, which they then develop. People spend extraordinary amounts of time building a life on these plots. (Isn't it incredible the way these people waste time?While you and I spend up to seventy hours a week working for firms we don't own and building futures we're not sure we'll enjoy, these people are designing and building things andmaking a life, even if only a virtual one. Scandalous!) They build houses — by designing and then constructing them — have family or friendsmove in, and pursue hobbies or raise pets. They may grow trees or odd plants — like Martha's. MMOG space grew out of "MUD" or "MOO" space. 6 MUDs and MOOs are virtual worlds, too, but they are text-based virtual worlds. There are no real graphics in aMUD orMOO, just text, reporting what someone says and does. You can construct objects inMOOspace and then have themdo things. But the objects act only through the mediation of text. (Their actions are generally quite simple, but even simple can be funny. One year, in a MUD that was part of a cyberlaw class, someone built a character named JPosner. If you poked JPosner, he muttered, "Poking is inefficient. " Another character was FEasterbrook. Stand in a room with FEasterbrook and use the word "fair," and FEasterbrook would repeat what you said, substituting the word "efficient. ""It's not fair" became "You mean, it's not efficient. ") Although it was easy for people who liked texts or who wrote well to understand the attraction of these text-based realities, it was not so easy for themany who didn't have that same fondness. MMOG space lifts that limit just a bit. It is themovie version of a cyberspace novel. You build things here, and they survive your leaving. You can build a house, and people walking down the street see it. You can let themcome in, and in coming into your house, they see things about you. They can see how you construct your world. If a particularMMOG space permits it, they might even see how you've changed the laws of the real world. In real space, for instance, people "slip and fall" on wet floors. In the MMOG space you've built, that "law"may not

exist. Instead, in your world, wet floors may make people "slip and dance. " The best example of this space today is the extraordinary community of Second Life. In it, people create both things and community, the avatars are amazingly well crafted, and their owners spend hundreds of thousands of hours building things in this space that others see, and some enjoy. Somemake clothes or hair styles, somemakemachines thatmakemusic. Whatever object or service the programming language allows, creators in Second Life are creating it. There aremore than 100,000 residents of Second Life at the time of this writing. They occupy close to 2,000 servers housed in downtown San Francisco, and suck 250 kilowatts of electricity just to run the computers — about the equivalent of 160 homes. But herewe get back toMartha andDank. In their exchange — whenMartha blamed Dank for having a dog that died with pain — they revealed what was most amazing about that particular MMOG. Martha's remarks ("Why do you have a dog that suffers when dying? Get yourself a pain-free-death dog, andmy petals will cause no harm") should have struck you as odd. You may have thought,"How weird that someone would think that the fault lay not in the poisonous petals but in a dog that died with pain. "But in this space,Dank did have a choice about how his dog would die. Maybe not a choice about whether "poison" would"kill" a dog, but a choice about whether the dog would"suffer"when it "died. "He also had a choice about whether a copy of the dog could be made, so that if it died it could be "revived. " InMMOGspace, these possibilities are not given by God. Or rather, if they are defined by God, then the players share the power of God. For the possibilities in MMOG space are determined by the code — the software, or architecture, that makes the MMOG space what it is. "What happens when" is a statement of logic; it asserts a relationship that is manifested in code. In real space we don't havemuch control over that code. In MMOG space we do. So, when Martha said what she said about the dog, Dank made what seemed tome an obvious response. "Why do your flowers have to stay poisonous once they leave your land?Why not make the petals poisonous only when on your land?When they leave your land — when, for example, they are blown onto my land — why not make them harmless?" It was an idea. But it didn't really help. ForMartha made her living selling these poisonous plants. Others (ok not many, but some) also liked the idea of this art tied to death. So it was no solution tomake poisonous plants that were poisonous only onMartha's property, unlessMartha was also interested in collecting a lot of very weird people on her land. But the idea did suggest another. "Okay," said Dank, "why not make the petals poisonous only when in the possession of someone who has 'purchased' them? If they are stolen, or if they blow away, then let the petals lose their poison. But when kept by the owner of the plant, the petals keep their poison. Isn't that a solution to the problem that both of us face?" The idea

was ingenious. Not only did it helpDank, it helpedMartha as well. As the code existed, it allowed theft. 7 (People want reality in that virtual space; there will be time enough for heaven when heaven comes.) But ifMartha could modify the code slightly so that theft8 removed a plant's poison, then "theft" would also remove the plant's value. That change would protect the profit in her plants as well as protect Dank's dogs. Here was a solution that made both neighbors better off — what economists call a pareto superior move. And it was a solution that was as possible as any other. All it required was a change of code. Think for a second aboutwhat's involved here. "Theft" entails (atminimum) a change in possession. But in MMOG space "possession" is just a relation defined by the software that defines the space. That same codemust also define the properties that possession yields. Itmight, like real space, distinguish between having a cake and eating it. Or itmight erase that distinction,meaning you can "eat"your cake, but once it's "eaten," itmagically reappears. InMMOGspace you can feed a crowd with five loaves and two fishes, and it isn't even amiracle. 9 So why not craft the same solution to Martha and Dank's problem?Why not define ownership to include the quality of poisonousness, and possession without ownership to be possession without poison? If the world is designed this way, then it could resolve the dispute between Martha and Dank, not by making one of them change his or her behavior, but by changing the laws of nature to eliminate the conflict altogether. We're a short way into this not so short book, though what I'mabout to say may make it a very short book indeed (for you at least). This book is all about the question raised by this simple story, and about any simplicity in this apparently simple answer. This is not a book about MMOG space or avatars. The story about Martha and Dank is the first and last example that will include avatars. But it is a book about cyberspace. My claim is that both "on the Internet" and "in cyberspace,"we will confront precisely the questions that Martha and Dank faced, as well as the questions that their solution raised. Both"on the Internet" and "in cyberspace," technology constitutes the environment of the space, and it will give us a much wider range of control over how interactions work in that space than in real space. Problems can be programmed or "coded" into the story, and they can be "coded" away. And while the experience with gamers so far is that they don't want virtual worlds to deviate too far from the real, the important point for now is that there is the capacity to make these worlds different. It is this capacity that raises the question that is at the core of this book:What does it mean to live in a world where problems can be coded away? And when, in that world, should we code problems away, rather than learn to work them out, or punish those who cause them? It is notMMOG space thatmakes these questions interesting problems for law; the very same problems will arise outside of MMOG space, and outside MUDs andMOOs. The problems of these

spaces are problems of the Internet in general. And asmore of our life becomes wired (and weird), in the sense that more of our life moves online, these questions will become more pressing. But I have learned enough in this business to know that I can't convince you of this with an argument. (I've spent the last 12 years talking about this subject; at least I know what doesn't work.) If you see the point, good for you. If you don't, I must show you. So my method for readers of the second sort must be more indirect. Proof, for them, will come in a string of stories, which aim to introduce and disorient. That, again, is the purpose of this chapter. Let me describe a few other places and the oddities that inhabit them.

GOVERNORS

A state — call it "Boral" — doesn't like its citizens gambling, even if many of its citizens do like gambling. But the state is the boss; the people have voted; the law is as it is. Gambling in the state of Boral is illegal. Then along comes the Internet.With the Net streaming into their homes through phones or cable lines, some citizens of Boral decide that Internet gambling is the next "killer app."A citizen of Boral sets up a "server" (a computer that is accessible on the Internet) that provides access to online gambling. The state doesn't like it. It tells this citizen, "Shut down your server or we will lock you up." Wise, if evasive, the gambling Boralian agrees to shut his server down — at least in the state of Boral. But he doesn't choose to leave the gambling business. Instead, he rents space on a server in an "offshore haven." This offshore web server hums away, once againmaking gambling available on theNet and accessible to the people of Boral via the Internet.Here's the important point: Given the architecture of the Internet (at least as it was circa 1999), it doesn't really matter where in real space the server is. Access doesn't depend on geography. Nor, depending on how clever the gambling sorts are, does access require that the user know anything about who owns, or runs, the real server. The user's access can be passed through anonymizing sites thatmake it practically impossible in the end to know *what* went on *where* and with whom. The Boral attorney general thus now faces a difficult problem. She may have moved the server out of her state, but she hasn't succeeded in reducing Boralian gambling. Before the Net, she would have had a group of people she could punish — those running gambling sites, and those who give those places custom. Now, the Net has made them potentially free from punishment — at the least because it is more difficult to know who is running the server or who is gambling. The world for this attorney general has changed. By going online, the gamblers moved into a world where this behavior is no longer *regulable*. By "regulable" I mean simply that a certain behavior is capable of regulation. The termis comparative, not absolute — in some place, at some time, a certain behavior will bemore regulable than at another place and in

another time. My claim about Boral is simply that the Net makes gambling less regulable there than it was before the Net.Or at least, in a sense that will become clearer as the story continues, with the architecture of the Net as it originally was, life on the Net is less regulable than life off the Net.

JAKE'S COMMUNITIES

If you hadmet Jake at a party inAnnArbor (were Jake at a party inAnnArbor), you would have forgotten him.10 If you didn't forget him, you might have thought, here's another quiet, dweeby University of Michigan undergraduate, terrified of the world, or, at least, of the people in the world. You wouldn't have figured Jake for an author — indeed, quite a famous short--story author, at least within his circles. In fact, Jake is not just a famous author, he was also a character in his own stories. But who he was in his stories was quite different from who he was in "real" life — if, that is, after reading his stories you still thought this distinction between "real life" and "not real life" made much sense. Jake wrote stories about violence — about sex as well, butmainly about violence. They seethed with hatred, especially of women. It wasn't enough to rape a woman, she had to be killed.And it wasn't enough that she was killed, she had to be killed in a particularly painful and tortured way. This is, however unfortunate, a genre of writing. Jake was a master of this genre. In real space Jake had quite successfully hidden this propensity. He was one of amillion boys: unremarkable, indistinguishable, harmless.Yet however inoffensive in real space, the harmfulness he penned in cyberspace was increasingly well known. His stories were published in USENET, in a group called alt.sex.stories. USENET isn't itself a network, except in the sense that the personal ads of a national newspaper are part of a network. Strictly speaking, USENET is the product of a protocol — a set of rules named the network news transfer protocol (NNTP) — for exchanging messages intended for public viewing. These messages are organized into "newsgroups," and the newsgroups are organized into subjects.Most of the subjects are quite technical,many are related to hobbies, and some are related to sex. Somemessages newsgroups come with pictures or movies, but some, like Jake's, are simply stories. There are thousands of newsgroups, each carrying hundreds of messages at any one time. Anyone with access to a USENET server can get access to the messages (or at least to the ones his administrator wants himto read), and anyone with access can post a message or respond to one already posted. Imagine a public bulletin board on which people post questions or comments. Anyone can read the board and add his or her own thoughts. Now imagine 15,000 boards, each with hundreds of "threads" (strings of arguments, each tied to the next). That, in any one place, is USENET. Now imagine these 15,000 boards, with hundreds of threads each, onmillions of computers across the world. Post amessage in one group, and it is added to

that group's board everywhere. That, for the world, is USENET. Jake, as I said, posted to a group called alt.sex.stories. "Alt" in that name refers to the hierarchy that the group sits within. Initially, there were seven primary hierarchies.11 "Alt" was created in reaction to this initial seven: Groups are added to the seven through a formal voting process among participants in the groups. But groups are added to "alt" based solely on whether administrators choose to carry them, and, generally, administrators will carry them if they are popular, as long as their popularity is not controversial. Among these groups that are carried only on demand, alt.sex.stories is quite popular.As with any writing space, if stories are "good" by the standards of the space — if they are stories that users of the space demand — they are followed and their authors become well known. Jake's stuff was very valuable in just this sense. His stories, about kidnapping, torturing, raping, and killing women,were as graphic and repulsive as any such story could be — which is why Jake was so famous among like-minded sorts. He was a supplier to these people, a constant and consistent fix. They needed these accounts of innocent women being violated, and Jake supplied them for free. One night in Moscow, a sixteen-year-old girl read a story by Jake. She showed it to her father, who showed it in turn to Richard DuVal, a Michigan alum. DuVal was shocked at the story, and angry that it bore the tag "umich.edu" on the story's header. He called his alma mater and complained. They took the complaint seriously.12 The university contacted the police; the police contacted Jake — with handcuffs and a jail cell. A slew of doctors examined him. Some concluded that he was a threat.The local prosecutors agreed with these doctors, especially after his computer was seized and e-mails were discovered between Jake and a Canadian fan who was planning to re-enact in real space one of the stories Jake published in cyberspace.At least, that's what the e--mails said.No one could tell for certain what the two men really intended. Jake said it was all pure fiction, and indeed, there was no evidence to prove otherwise. Nonetheless, federal charges were brought against Jake for the transmission of a threat. Jake said that his stories were only words, protected by the First Amendment to the U.S.Constitution.Amonth and a half later, a court agreed. The charges were dropped,13 and Jake returned to the special kind of obscurity that had defined his life before. I don't care so much just now about whether Jake Baker's words should have been protected by the Constitution. My concern is Jake Baker himself, a person normed into apparent harmlessness in real space, but set free in cyberspace to become the author of this violence. People said Jake was brave, but he wasn't "brave" in real space. He didn't express his hatred in classes, among friends, or in the school newspaper. He slithered away to cyberspace, and only there did his deviancy flourish. He did this because of something about him and something about cyberspace. Jake was the sort who wanted to spread stories of violence, at le-

ast if he could do so without public account. Cyberspace gave Jake this power. Jake was in effect an author and publisher in one.He wrote stories, and as quickly as he finished them he published them — to some thirty million computers across the world within a few days. His potential audience was larger than twice that for the top fifteen best-selling novels combined, and though he made nothing fromhis work, the demand for it was high. Jake had discovered a way tomainline his depravity into the veins of a public for whom this stuff was otherwise quite difficult to find. (Even *Hustler* wouldn't publish the likes of this.) Of course, there were other ways Jake could have published. He could have offered his work to*Hustler,* or worse. But no real-world publication would have given Jake a comparable audience. Jake's readership was potentially millions, stretching across country and continent, across culture and taste. This reach was made possible by the power in the network: Anyone anywhere could publish to everyone everywhere. The network allowed publication without filtering, editing, or, perhaps most importantly, responsibility. One could write what one wanted, sign it or not, post it to machines across the world, and within hours the words would be everywhere.The network removed themost important constraint on speech in real space — the separation of publisher fromauthor.There is vanity publishing in real space, but only the rich can use it to reach a broad audience. For the rest of us, real space affords only the access that the publishers want to give us. Thus cyberspace is different because of the reach it allows. But it is also different because of the relative anonymity it permits. Cyberspace permitted Jake to escape the constraints of real space. He didn't "go to" cyberspace when he wrote his stories, in the sense that he didn't "leave"Ann Arbor. But when he was "in" cyberspace, it allowed him to escape the norms of Ann Arbor.He was free of real-life constraints, of the norms and understandings that had successfully formed himinto amember of a college community.Maybe he wasn't perfectly at home;maybe he wasn't the happiest. But the world of theUniversity of Michigan had succeeded in steering him away from the life of a psychopath — except when it gave him access to the Net.On the Net he was someone else. As the Internet has grown, it has produced many more opportunities for Jake-like characters — characters that do things in the virtual world that they would never do in the real world. One of the most popular MMOGs is a game called "Grand Theft Auto." In this game, one practices committing crimes.And one of themost troubling uses of video chat is the practice of virtual — prostitution by children.As the *New York Times* recently reported, thousands of children spend hundreds of hours prostituting themselves online. Sitting in the "privacy" of their own bedroom, using the iSight camera their parents gave them for Christmas, a 13-year-old girl or boy enacts the sexual behavior demanded by the audience. The audience gets their fix of sexual perversion. The kid gets money, and whatever psychological baggage

this behavior creates.14 It is impossibly difficult to look across this range of Jake-like characters and not think that, at some point, the virtual has crossed over into something real. Or, at least, the virtual has real effects — either on those who live it, or on those who live with them.15When Jake was prosecuted,many FirstAmendment defenders argued his words, however vivid, never crossed into reality. And no doubt, there is a difference between writing about rape and raping, just as there is a difference between an actor enacting rape and actually raping someone. But I take it that all concede a line is crossed somewhere as wemove across this range of Jake-like characters. If a parent was untroubled by the virtual prostitution of her son in his bedroom,we would not understand that to be principled free speech activism, even if the only "prostitution" was the son describing in text how he was molested by those in the chat. But my point is not to draw lines between the acceptable virtual dual-lives and the unacceptable. It is instead to remark that this space enablesmore of this duality.And though part of this duality is always "only virtual," and sometimes "only words," real-space regulators (whether parents or governments) will feel compelled to react. The Net enables lives that were previously impossible, or inconvenient, or uncommon.At least some of those virtual lives will have effects on non-virtual lives — both the lives of the people living in the virtual space, and the lives of those around them.

WORMS THAT SNIFF

A"worm" is a bit of computer code that is spit out on theNet and works its way into the systems of vulnerable computers. It is not a "virus" because it doesn't attach itself to other programs and interfere with their operation. It is just a bit of extra code that does what the code writer says. The code could be harmless and simply sit on someone'smachine.Or it could be harmful and corrupt files or do other damage that its author commands. Imagine a worm designed to do good (at least in the minds of some). Imagine that the code writer is the FBI and that the FBI is looking for a particular document belonging to the National Security Agency (NSA). Suppose that this document is classified and illegal to possess without the proper clearance. Imagine that the wormpropagates itself on the Net, finding its way onto hard disks wherever it can.Once on a computer's hard disk, it scans the entire disk. If it finds the NSA document, it sends amessage back to the FBI saying as much. If it doesn't, it erases itself. Finally, assume that it can do all this without "interfering" with the operation of the machine. No one would know it was there; it would report back nothing except that the NSA document was on the hard disk. Is this an unconstitutional worm? This is a hard question that at first seems to have an easy answer. The wormis engaging in a government-initiated search of citizens' disks. There is no reasonable suspicion (as the law

ordinarily requires) that the disk holds the document for which the government is searching. It is a generalized, suspicionless search of private spaces by the government. Fromthe standpoint of the Constitution — the Fourth Amendment in particular — you don't get any worse than that. The Fourth Amendment was written against the background of just this sort of abuse. Kings George II and George III would give officers a "general warrant" authorizing them to search through private homes looking for evidence of a crime.16 No suspicion was needed before the officer ransacked your house, but because he had a warrant, you were not able to sue the officer for trespass. The aimof the Fourth Amendment was to require at least suspicion, so that the burden of the search fell on a reasonably chosen class.17 But is the wormreally the same as the King's general search?One important difference is this: Unlike the victims of the general searches that the Framers of our Constitution were concerned about, the computer user never knows that his or her disk is being searched by the worm.With the general search, the police were breaking into a house and rummaging through private stuff. With the worm, it is a bit of computer code that does the breaking, and (I've assumed) it can "see" only one thing. And perhaps more importantly, unlike the general search, the wormlearns little and leaves no damage after it's finished: The code can't read private letters; it doesn't break down doors; it doesn't interfere with ordinary life.And the innocent have nothing to fear. The wormis silent in a way that King George's troops were not. It searches perfectly and invisibly, discovering only the guilty. It does not burden the innocent; it does not trouble the ordinary citizen; it captures only what is outside the protection of the law. This difference complicates the constitutional question.The worm's behavior is like a generalized search in that it is a search without suspicion. But it is unlike the historical generalized search in that it creates no disruption of ordinary life and "discovers" only contraband. In this way, the worm is like a dog sniff — which at least at airports is constitutionally permissible without probable cause18 — but better. Unlike the dog sniff, the worm doesn't even let the computer user know when there is a search (and hence the user suffers no particularized anxiety). Is the worm, then, constitutional? That depends on your conception of what the Fourth Amendment protects. In one view, the amendment protects against suspicionless governmental invasions,whether those invasions are burdensome or not. In a second view, the amendment protects against invasions that are burdensome, allowing only those for which there is adequate suspicion that guilt will be uncovered. The paradigm case that motivated the framers does not distinguish between these two very different types of protections, because the technology of the time wouldn't distinguish either.You couldn't — technically — have a perfectly burdenless generalized search in 1791. So they didn't — technically — express a view about whether such a search

should be constitutionally proscribed. It is instead we whomust choose what the amendment is to mean. Let's take the example one step further. Imagine that the worm does not search every machine it encounters, but instead can be put on a machine only with judicial authorization — say, a warrant.Now the suspicionless-search part of the problem has been removed. But now imagine a second part to this rule: The government requires that networks be constructed so that a worm, with judicial authorization, could be placed on any machine. Machines in this regime, in other words,must bemade worm--ready, even though worms will be deployed only with judicial warrant. Is there any constitutional problem with this? I explore this question in much greater detail in Chapter 11, but for now, notice its salient feature. In both cases,we are describing a regime that allows the government to collect data about us in a highly efficient manner — inexpensively, that is, for both the government and the innocent. This efficiency is made possible by technology, which permits searches that before would have been far too burdensome and invasive. In both cases, then, the question comes to this: When the ability to search without burden increases, does the government's power to search increase as well? Or,more darkly, as James Boyle puts it: "Is freedom inversely related to the efficiency of the available means of surveillance?" For if it is, as Boyle puts it, then "we have much to fear."19 This question, of course, is not limited to the government.One of the defining features of modern life is the emergence of technologies that make data collection and processing extraordinarily efficient.Most of what we do — hence, most of what we are — is recorded outside our homes. When you make telephone calls, data are recorded about whom you called, when, how long you spoke, and how frequently you made such calls.20 When you use your credit cards, data are recorded about when, where, what, and from whom you made purchases. When you take a flight, your itinerary is recorded and possibly profiled by the government to determine whether you are likely to be a terrorist.21 If you drive a car in London, cameras record your license plate to determine whether you've paid the proper "congestion tax."No doubtHollywood's image of counter-terrorist units — where one person sitting behind a terminal instantly tracks the life of another — is wrong. But it need not be terribly wrong formuch longer. Itmay not be easy to imagine systems that follow an individual wherever he goes, but it is easy to imagine technologies that gather an extraordinary amount of data about everything we do andmake those data accessible to those with the proper authorization.The intrusiveness would be slight, and the payoff could be great. Both private and public monitoring in the digital age, then, have the same salient feature: monitoring, or searching, can increase without increasing the burden on the individual searched. Both present a similar question:How should we think about this change? How

should the protection the framers gave us be applied to a world the framers couldn't even imagine?

THEMES

Four stories, four themes, each a window into one aspect of cyberspace that will be central in all that follows. My aim in the balance of this book is to work through the issues raised by these four themes. I thus end this chapter with a map of the four, laid out in the order they will appear in the balance of the book. That order begins with story number two. Regulability "Regulability" is the capacity of a government to regulate behavior within its proper reach. In the context of the Internet, thatmeans the ability of the government to regulate the behavior of (at least) its citizens while on the Net. The story about Boral was thus a story about regulability, ormore specifically, about the changes in regulability that cyberspace brings. Before the Internet, it was relatively easy for the attorney general of Boral to control commercial gambling within her jurisdiction; after the Internet, when the servers moved outside of Boral, regulation became much more difficult. For the regulator, this is just a particular instance of a much more general story. To regulate well, you need to know (1) who someone is, (2) where they are, and (3) what they're doing. But because of the way the Internet was originally designed (andmore on this below), there was no simple way to know (1) who someone is, (2) where they are, and (3) what they're doing. Thus, as life moved onto (this version of) the Internet, the regulability of that life decreased. The architecture of the space — at least as it was — rendered life in this space less regulable. The balance of Part I is about regulability.Can we imagine amore regulable cyberspace? Is this the cyberspace we are coming to know? Regulation by Code The story about Martha and Dank is a clue to answering this question about regulability. If inMMOG space we can change the laws of nature — make possible what before was impossible, or make impossible what before was possible — why can't we change regulability in cyberspace?Why can't we imagine an Internet or a cyberspace where behavior can be controlled because code now enables that control? For this, importantly, is just whatMMOG space is.MMOG space is "regulated," though the regulation is special. In MMOG space regulation comes through code. Important rules are imposed, not through social sanctions, and not by the state, but by the very architecture of the particular space. A rule is defined, not through a statute, but through the code that governs the space. This is the second theme of this book: There is regulation of behavior on the Internet and in cyberspace, but that regulation is imposed primarily through code. The differences in the regulations effected through code distinguish different parts of the Internet and cyberspace. In some places, life is fairly free; in other places, it is more controlled. And the difference between these spaces is simply a difference in

the architectures of control — that is, a difference in code. If we combine the first two themes, then, we come to a central argument of the book: The regulability described in the first theme depends on the code described in the second. Some architectures of cyberspace aremore regulable than others; some architectures enable better control than others. Therefore, whether a part of cyberspace — or the Internet generally — can be regulated turns on the nature of its code. Its architecture will affect whether behavior can be controlled. To follow Mitch Kapor, its architecture is its politics.22 And from this a further point follows: If some architectures are more regulable than others — if some give governmentsmore control than others — then governments will favor some architectures more than others. Favor, in turn, can translate into action, either by governments, or for governments. Either way, the architectures that render space less regulable can themselves be changed tomake the spacemore regulable. (By whom, and why, is amatter we take up later.) This fact about regulability is a threat to those who worry about governmental power; it is a reality for those who depend upon governmental power. Some designs enable governmentmore than others; some designs enable government differently; some designs should be chosen over others, depending upon the values at stake.

BIBLIOGRAFIA ADICIONAL

BERG, Terrence. www.wildwest.gov: The impact of the Internet on state power to enforce the law. Brigham Young University Law Review, 2000.

CASTELLS, Manuel. Infomationalism, Networks, and the Network Society: A Theoretical Blueprint. In: CASTELLS, Manuel (Org.). The network society: a cross-cultural perspective. Cheltenham: Edward Elgar, 2004.

REIDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. Texas Law Review, 76, 1998.

RHEINGOLD, Howard. The virtual community: homesteading on the electronic frontier. Cambridge (MA): The MIT Press, 2000.

ZITTRAIN, Jonathan. The Future of the Internet and How to Stop It. New Haven: Yale University Press, 2008.

WU, Tim. When code isn't law. Virginia Law Review, 89, 2003.

CAPÍTULO 2 — LIBERDADE DE EXPRESSÃO E ACESSO À INTERNETS

A) LIBERDADE DE EXPRESSÃO E ACESSO À INTERNET NO ESTRANGEIRO

Suprema Corte dos Estados Unidos
RENO V. ACLU, 521 U.S. 844 (1997)
Informações básicas:
http://edition.cnn.com/US/9706/26/cda.overturned.hfr/index.html?eref=sitesearch

Resumo da situação

"Two provisions of the Communications Decency Act of 1996 (CDA or Act) seek to protect minors from harmful material on the Internet, an international network of interconnected computers that enables millions of people to communicate with one another in "cyberspace" and to access vast amounts of information from around the world. Title 47 U. S. C. A. § 223(a)(1)(B)(ii) (Supp. 1997) criminalizes the "knowing" transmission of "obscene or indecent" messages to any recipient under 18 years of age. Section 223(d) prohibits the "knowin[g]" sending or displaying to a person under 18 of any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Affirmative defenses are provided for those who take "good faith,... effective... actions" to restrict access by minors to the prohibited communications, § 223(e)(5)(A), and those who restrict such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number, (…) The Government appealed to this Court under the Act's special review provisions, arguing that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague."

O que está em questão?

"The CDA's "indecent transmission" and "patently offensive display" provisions [violate] "the freedom of speech" protected by the First Amendment."

Decisão — Voto do Justice Stevens

"At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment. [n1]

(…)

The Internet is "a unique and wholly new medium of worldwide human communication." [n4]

(…)

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium--known to its users as "cyberspace"--located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

(…)

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. [n9] Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web." [n10]

(…)

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest core." [n11] These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community." [n12]

(…)

Though such material is widely available, users seldom encounter such content accidentally. "A document's title or a description of the document will usually appear before the document itself... and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content." [n15] For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident. [n16]

(…)

The first, 47 U. S. C. A. § 223(a) (Supp. 1997), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

'(a) Whoever (…) (B) by means of a telecommunications device knowingly (…) (i) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication (…) shall be fined under Title 18, or imprisoned not more than two years, or both.'

The second provision, § 223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

'(d) Whoever (1) in interstate or foreign communications knowingly (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; (…) shall be fined under Title 18, or imprisoned not more than two years, or both.'

(…)

The judgment of the District Court enjoins the Government from enforcing the prohibitions in § 223(a)(1)(B) insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein.

(…) In its appeal, the Government argues that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad (…)

The CDA fails to provide us with any definition of the term "indecent" as used in § 223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by § 223(d) lack serious literary, artistic, political, or scientific value.

(…)

there are significant differences between the order upheld in Pacifica and the CDA. First, the order in Pacifica, issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when--rather than whether--it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet. Second, unlike the CDA, the Commission's declaratory order was not punitive; we expressly refused to decide whether the indecent broadcast "would justify a criminal prosecution." Id., at 750. Finally, the Commission's order applied to a medium which as a matter of history had "received the most limited First Amendment protection," i d., at 748, in large part because warnings could not adequately protect the listener from unexpected program content. The Internet, however, has no comparable history. Moreover, the District Court found that the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material.

(…) According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content based blanket restriction on speech (…)

These precedents, then, surely do not require us to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

(…)

Finally, unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low cost capacity for communication of all kinds. The Government estimates that "[a]s many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." [n34] This dynamic, multifa-

ceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought." 929 F. Supp., at 842 (finding 74). We agree with its conclusion (…)

The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. (…) Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. (…) As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns (…)

In contrast to Miller and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

(…)

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in Ginsberg and Pacifica, the scope of the CDA is not limited to commercial speech or commercial entities. Its open ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. [n44] Moreover, the "community standards" criterion as applied to the

Internet means that any communication available to a nation wide audience will be judged by the standards of the community most likely to be offended by the message. [n45] (…) It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library.

(…)

As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

For the foregoing reasons, the judgment of the district court is affirmed.

CONSELHO CONSTITUCIONAL DA FRANÇA

Decision n° 2009-580 of June 10th 2009
Informações básicas:
http://www1.folha.uol.com.br/folha/informatica/ult124u579424.shtml
--

Decision n° 2009-580 of June 10th 2009 Act furthering the diffusion and protection of creation on the Internet th A referral was made to the Constitutional Council on May 19 2009, pursuant to Article 61, paragraph 2 of the Constitution, by Messrs Jean-Marc AYRAULT et al., Members of the National Assembly, with respect to the Act furthering the diffusion and protection of creation on the Internet

(…)

4. Firstly section 5 of the statute referred for review inserts into Chapter 1 of Title III of Book III of the first part of the Intellectual Property Code a section comprising Articles L 331-12 to L 331-45 devoted to the "High Authority for the diffusion of works and protection of copyright on the Internet". This new independent administrative authority is composed of a college and a committee for the protection of copyright. The college is responsible in particular for furthering the lawful offer of works and property covered by copyright or related rights. The task of the Committee for the protection of copyright is to trigger the new warning mechanisms and administrative penalties incurred by internet users who have failed to monitor access to the internet. 5. Secondly, section 11 inserts into Chapter IV of the same Title Articles L 336-3 and L 336-4. It defines the duty to monitor access to the internet and determines the cases in which internet subscribers whose access has been used in a manner such as to infringe copyright will escape the imposition of penalties.

(…)

— As regards the duty to monitor access to the internet: 6. The first paragraph of Article L336-3 of the Intellectual Property Code provides "A person who has subscribed to internet access to online public communication services is under a duty to ensure that said access is not used for reproducing, showing, making available or communicating to the public works or property protected by copyright or a related right without the authorization of the copyright holders provided for in Books I and II when such authorization is required".

9. Secondly, under Article L 331-27: "When it has been ascertained that the subscriber has failed to comply with the duty defined in Article L 336-3 in the year following receipt of a recommendation addressed by the Committee for the protection of copyright accompanied by a signed acknowledgment of receipt or any other means likely to prove the date of the sending

of said recommendation and its receipt by the subscriber, the Committee may, after a full hearing of all parties, impose one of the following penalties depending on the seriousness of the failure to comply and the use of internet access: 1° Suspension of access to the Internet for a period of between two months and one year accompanied by the impossibility for the subscriber to enter into any other contract with any other operator for access to online public communication services

(…)

10. Under Article L 331-28, the High Authority's Committee for the protection of copyright may, before initiating penalty proceedings, propose an amicable arrangement whereby the offending subscriber has his/her internet access cut off for a period of between one to three months, or is put under a duty to take the necessary steps to prevent the re-occurrence of said breach of duty.

(…)

11. The parties contend that by giving an administrative authority, albeit independent, the power to impose penalties in the form of withholding access to the internet, Parliament firstly infringed the fundamental right of freedom of expression and communication, and secondly, introduced patently disproportionate penalties.

(…)

12. Article 11 of the Declaration of the Rights of Man and the Citizen of 1789 proclaims: "The free communication of ideas and opinions is one of the most precious rights of man. Every citizen may thus speak, write and publish freely, except when such freedom is misused in cases determined by Law". In the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services.

(…)

16. The powers to impose penalties created by the challenged provisions vest the Committee for the protection of copyright, which is not a court of law, with the power to restrict or deny access to the internet by access holders and those persons whom the latter allow to access the internet. The powers vested in this administrative authority are not limited to a specific category of persons but extend to the entire population. The powers of this Committee may thus lead to restricting the right of any person to exercise his right to express himself and communicate freely, in particular from his own home. In these conditions, in view of the freedom guaranteed by Article 11 of the Declaration of 1789, Parliament was not at liberty, irrespective of the guarantees accompanying the imposition of penalties, to vest an administrative

authority with such powers for the purpose of protecting holders of copyright and related rights;

(…)

18. In the case in hand, under the provisions referred for review, the commission of an infringement of copyright at the address of the registered subscriber constitutes, according to the terms of the second paragraph of Article L 331-21 "the material ingredients of the breach of duty defined in Article L 336-3". Solely the party to the internet access contract may be the object of the penalties introduced by the provisions referred for review. In order to avoid the imposition of such penalties it is incumbent upon him, under Article L 331-38, to adduce evidence that the infringement of copyright or related rights was due to fraud perpetrated by a third party. Thus by reversing the burden of proof, Article L 331-38, introduces, contrary to the requirements deriving from Article 9 of the Declaration, a presumption of guilt on the part of the internet access holder such as to entail the imposition of penalties restricting or depriving him of his rights.

(…)

Deliberated by the Constitutional Council sitting on June 10th 2009 and composed of Messrs Jean-Louis DEBRE, President, Guy CANIVET, Jacques CHIRAC, Renaud DENOIX de SAINT MARC and Olivier DUTHEILLET de LAMOTHE, Mrs Jacqueline de GUILLENCHMIDT, Messrs Pierre JOXE and Jean-Louis PEZANT, Mrs Dominique SCHNAPPER and Mr Pierre STEINMETZ.

Bibliografia Adicional

BALKIN, Jack. Digital speech and democratic culture: a theory of freedom of expression for the information society. New York University Law Review. V. 79, n. 1, p. 1-58. abr 2004.

BELL, Daniel. The social framework of the information society. in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

DIMAGGIO, Paul; HARGITTAI, Eszter; NEUMAN, W. Russell; ROBINSON, John P. Social implications of the internet. in: MANSELL, Robin (Org.). The information society. v. IV (Everyday life). New York: Routledge, 2009.

HARTMANN, Ivar A. M. A Right to Free Internet? On Social Rights and Internet Access. Journal of High Technology Law, vol. XIII, n. 2, 2013.

KUGELMANN, Dieter. Informationsfreiheit als Element moderner Staatlichkeit. DöV. v. 20, 2005.

LICOPPE, Christian; SMOREDA, Zbigniew. Rhythms and ties. Toward a pragmatics of technologically mediated sociability. in: KRAUT, Robert; BRYNIN, Malcolm; KIESLER, Sara (Orgs.). Computers, phones, and the internet: domesticating information technology. Oxford: Oxford Univ. Press, 2006.

B) LIBERDADE DE EXPRESSÃO NO BRASIL

Superior Tribunal de Justiça

Recurso Especial No. 1193764
Informações básicas:
http://www.migalhas.com.br/Quentes/17,MI125068,11049-STJ+Google+nao+pode+ser+responsabilizado+por+material+publicado+no

Voto da Min. Nancy Andrighi

Ação: de obrigação de fazer cumulada com indenização por danos morais, ajuizada pela recorrente em desfavor de GOOGLE BRASIL INTERNET LTDA., sob a alegação de ter sido alvo de ofensas em página na internet da comunidade ORKUT, mantida pelo GOOGLE.

Houve a concessão de tutela antecipada, para o fim de determinar a "exclusão de todo o material ofensivo que relacione o nome da autora" (fl. 148, e-STJ).

Sentença: julgou parcialmente procedentes os pedidos iniciais, apenas para tornar definitivos os efeitos da tutela, no entanto sem a condenação do GOOGLE ao pagamento de indenização por danos morais (fls. 201/211, e-STJ).

Acórdão: o TJ/SP negou provimento ao apelo da recorrente, nos termos do acórdão (fls. 285/288, e-STJ) assim ementado: "Obrigação de fazer — Provedor de hospedagem "Orkut" — Não se equipara o provedor a editor ou diretor de jornal ou de revista por notícias divulgadas em "home page" de usuários apenas abrigados em seu sistema — Ausência de qualquer ilicitude na conduta da apelada e inexistência do necessário nexo de implicação entre os danos morais apontados e a ação da demanda — Recurso improvido."

(...)

Na hipótese específica do ORKUT, comunidade virtual na qual foram veiculadas as informações tidas por ofensivas, verifica-se que o GOOGLE atua como provedor de conteúdo, pois o site disponibiliza informações, opiniões e comentários de seus usuários. Estes usuários criam páginas pessoais (perfis), por meio das quais se relacionam com outros usuários e integram grupos (comunidades), igualmente criados por usuários, nos quais se realizam debates e troca de informações sobre interesses comuns.

(...)

Não obstante a indiscutível existência de relação de consumo no serviço prestado por intermédio do ORKUT, a responsabilidade do GOOGLE deve ficar restrita à natureza da atividade por ele desenvolvida naquele site, que, a partir do quanto visto linhas acima, corresponde à típica provedoria de

conteúdo, disponibilizando na rede as informações encaminhadas por seus usuários.

Nesse aspecto, o serviço do GOOGLE deve garantir o sigilo, a segurança e a inviolabilidade dos dados cadastrais de seus usuários, bem como o funcionamento e a manutenção das páginas na internet que contenham as contas individuais e as comunidades desses usuários.

No que tange à fiscalização do conteúdo das informações postadas por cada usuário, não se trata de atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra o material nele inserido.

(...)

Ademais, o controle editorial prévio do conteúdo das informações se equipara à quebra do sigilo da correspondência e das comunicações, vedada pelo art. 5º, XII, da CF/88. Não bastasse isso, a verificação antecipada, pelo provedor, do conteúdo de todas as informações inseridas na web eliminaria — ou pelo menos alijaria — um dos maiores atrativos da internet, que é a transmissão de dados em tempo real.

(...)

Em outras palavras, exigir dos provedores de conteúdo o monitoramento das informações que veiculam traria enorme retrocesso ao mundo virtual, a ponto de inviabilizar serviços que hoje estão amplamente difundidos no cotidiano de milhares de pessoas. A medida, portanto, teria impacto social e tecnológico extremamente negativo.

Mas, mesmo que, ad argumentandum, fosse possível vigiar a conduta dos usuários sem descaracterizar o serviço prestado pelo provedor, haveria de se transpor outro problema, de repercussões ainda maiores, consistente na definição dos critérios que autorizariam o veto ou o descarte de determinada informação. Ante à subjetividade que cerca o dano moral, seria impossível delimitar parâmetros de que pudessem se valer os provedores para definir se uma mensagem ou imagem é potencialmente ofensiva. Por outro lado, seria temerário delegar o juízo de discricionariedade sobre o conteúdo dessas informações aos provedores. Por todos esses motivos, não vejo como obrigar do GOOGLE a realizar a prévia fiscalização do conteúdo das informações que circulam no ORKUT.

(...)

Em suma, pois, tem-se que os provedores de conteúdo: (i) não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem

manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso.

Ainda que não ideais, certamente incapazes de conter por completo a utilização da rede para fins nocivos, a solução ora proposta se afigura como a que melhor equaciona os direitos e deveres dos diversos players do mundo virtual.

(...)

A recorrente interpôs a presente ação objetivando compelir o GOOGLE a suprimir do ORKUT texto cujo conteúdo considerava ofensivo à sua pessoa, bem como para ser indenizada pelos respectivos danos morais.

Houve a concessão de tutela antecipada, para o fim de determinar a "exclusão de todo o material ofensivo que relacione o nome da autora" (fl. 148, e-STJ), tendo o GOOGLE prontamente dado cumprimento à ordem judicial, esclarecendo que a comunidade onde estavam sendo veiculadas as informações "foi removida em 28 de abril do corrente ano" (fl. 195, e-STJ).

Nesse ponto, portanto, não houve ilegalidade nos atos praticados pelo GOOGLE que, uma vez ciente da existência de material de conteúdo ofensivo, adotou todas as providências tendentes à sua imediata remoção do site.

(...)

Portanto, não se vislumbra responsabilidade do GOOGLE pela veiculação das mensagens cujo conteúdo a recorrente considerou ofensivo à sua moral. Forte nessas razões, NEGO PROVIMENTO ao recurso especial.

Tribunal de Justiça do Distrito Federal

Apelação 20090110667444APC
3ª. Turma Cível
Informações básicas:
http://www.tjdft.jus.br/institucional/imprensa/noticias/2013/setembro/consumidor-e-condenado-a-indenizar-por-abuso-no-direito-de-reclamar

Ementa
CIVIL E PROCESSUAL CIVIL. AÇÃO DE INDENIZAÇÃO. PRESTAÇÃO DE SERVIÇOS. CURSO PROFISSIONALIZANTE. INSATISFAÇÃO POR PARTE DO ALUNO. RECLAMAÇÃO PÚBLICA NA INTERNET. ABUSO DE DIREITO. EXCESSO DO RECLAMANTE. DANOS MORAIS. CONFIGURAÇÃO. PEDIDO RECONVENCIONAL. IMPROCEDÊNCIA.
R E L A T Ó R I O
Cuida-se de Apelação Cível interposta por PAULO VINICIUS DE JESUS MADEIRA BASTOS, em face da r. sentença exarada às fls. 270/277.
Na origem, VALIO EDUCAÇÃO PROFISSIONAL LTDA, ROMERO VILHENA VÁLIO e CAROLINA LUDWIG VÁLIO MARCOMINI ajuizaram Ação de Indenização por Danos Morais, com pedido cumulado de obrigação de fazer, em face do ora apelante, alegando que o réu realizou curso básico de tratamento de imagem e que, após o recebimento do certificado, manifestou insatisfação com o serviço que lhe foi prestado, requerendo a devolução dos valores pagos, o que lhe foi negado.
Os autores afirmaram que, na prática, o réu objetivava "receber um serviço sem dar sua contraprestação", e que já na época do curso tentava intimidar a empresa, pois se gabava por ser o campeão de reclamações junto ao PROCON.
Prosseguiram os autores afirmando que o réu veiculou uma reclamação pública em face da empresa autora no sítio eletrônico "Reclame Aqui" (www.reclameaqui.com.br), em que "cita de forma difamatória, caluniosa e ofensiva todos os Requerentes", e que também protocolou reclamação junto ao PROCON do Distrito Federal, onde também teriam sido ditas diversas mentiras contra a empresa requerente.
Assim, os autores requereram a condenação do réu à obrigação de excluir a reclamação existente no situo eletrônico "Reclame Aqui", bem como ao pagamento de indenização por danos morais, no importe de 15 (quinze mil reais).
(...)
A d. Magistrada sentenciante julgou improcedente o pleito reconvencional e julgou parcialmente procedente o pedido deduzido na inicial, para condenar o réu/reconvinte a retirar a reclamação registrada no sítio eletrônico

"Reclame Aqui", bem como ao pagamento de indenização por danos morais causados, na quantia de R$ 9.000,00 (nove mil reais), bem como ao pagamento dos ônus de sucumbência.

Voto da Desa. Nídia Corrêa Lima

A meu ver, não há como ser a controvérsia julgada sob o aspecto da qualidade dos serviços prestados pela empresa autora, como pretende o réu, uma vez que a análise de qualidade não estaria sendo pautada em critérios objetivos, mas sim na opinião parcial do réu ou de terceiros sobre um curso realizado há vários anos (no ano de 2009).

De qualquer sorte, ainda que fosse considerado tal fato, não poderiam ser desconsideradas as opiniões dos demais alunos que freqüentaram o mesmo curso que o réu e que, àquela época, avaliaram positivamente o instituto e o curso ministrado pela empresa ré (fls. 33 a 40).

(...)

Não bastasse o disposto no material publicitário, o contrato firmado entre as partes prevê expressamente que o material didático não incluía disquetes Cd´s ou mídias.

(...)

Percebe-se, dessa forma, que não assiste razão ao apelante, ao afirmar que foi induzido a acreditar que o serviço contratado incluía o fornecimento de CD, CD Corel Draw, Cd Indesign e de qualquer outro material além da apostila que lhe foi entregue.

Impõe-se verificar, portanto, se na reclamação formalizada junto ao sítio eletrônico "Reclame Aqui", o réu/apelante se limitou a manifestar a insatisfação pelos serviços que lhe foram prestados pela empresa autora e pelo tratamento que lhe foi dispensado pelos demais autores ou se ultrapassou os limites da razoabilidade e fez uso de termos difamatórios.

Assim como os fornecedores podem cadastrar os maus pagadores em bancos de restrição ao crédito — a fim de alertar os demais credores sobre o risco a que se sujeitam quando negociam com uma pessoa com histórico de inadimplência — também há direito aos consumidores de se informarem quanto aos prestadores de serviços que deixam de cumprir suas obrigações.

Na falta de um órgão atuante, empresas e sítios particulares passaram a cumprir o papel do Estado na prestação deste importante serviço aos consumidores, mantendo cadastros sobre os níveis de inadimplência dos fornecedores e sobre o grau de insatisfação dos consumidores com cada empresa atuante no mercado de consumo.

O registro de reclamações nas redes sociais e em sites especializados virou uma importante ferramenta de autocontrole do mercado. Hoje, consumidores se informam mais antes de consumir e as empresas, preocupadas com a repercussão das reclamações publicadas pelos seus consumidores, se preo-

cupam mais em solucionar voluntariamente os problemas causados por seus produtos ou serviços.

Ocorre que, no presente caso, a manifestação formulada pelo réu (fls. 41/42) evidencia inequívoco excesso de sua parte, visto que este não se limita a alertar os demais consumidores quanto à sua insatisfação com a qualidade do curso oferecido pela empresa autora.

O apelante afirma que o material publicitário promete a entrega de Livro Photoshop 3 e de CD, o que, conforme visto anteriormente, não é verdade. A propaganda do curso realizado pelo réu não sugere a entrega de tal material, pois esclarece expressamente que o material didático é exclusivo e próprio.

Ademais, o réu teceu uma série de outros comentários que não dizem respeito à qualidade do curso, afirmando, por exemplo, que a empresa ré consiste em uma "máfia" e que as funcionárias Carolina e Marília são "assessoras — travestidas-de-dobermans" do "(ir)responsável Romero".

O réu ainda chama a autora Carolina de "doberman com pedigree de pitbull" e, ao final, afirma que iria ao PROCON para ver se lá os funcionários da empresa autora teriam a coragem de praticar "a patifaria, a canalhice, a safadeza e a desonestidade que tiveram ao prometer uma coisa" que não teria sido cumprida.

Assim, entendo configurado o excesso por parte do réu/apelado, ao manifestar o seu inconformismo com a qualidade de um serviço que teria sido prestado, que atingiram a honra dos autores, mostrando-se cabível a indenização vindicada na inicial.

(...)

No caso em apreço, o réu se excedeu ao manifestar sua insatisfação quanto ao curso realizado, tratando a imagem da empresa e dos demais autores com escárnio e os expondo desnecessariamente a constrangimento perante o mercado consumidor.

(...)

Pelas razões expostas, NEGO PROVIMENTO AO RECURSO e mantenho íntegra a r. sentença. É como voto.

Bibliografia Adicional

DIMOULIS, Dimitri. O direito de ofender: sobre os limites da liberdade de expressão artística. Revista Brasileira de Estudos Constitucionais — RBEC, v. 3, n. 10, p. 49-65, abr./jun. 2009.

MEYER-PFLUG, Samantha Ribeiro. Liberdade de expressão e discurso do ódio: racismo, discriminação, preconceito, pornografia, financiamento pú-

blico das atividades artísticas das campanhas eleitorais. São Paulo: Revista dos Tribunais, 2009.

SANTOS, Gustavo Ferreira. Da liberdade de expressão ao direito à comunicação. Direitos Fundamentais & Justiça, v. 10, p. 200-204, 2010.

CAPÍTULO 3 — PRIVACIDADE E DADOS PESSOAIS

A) PROTEÇÃO DE DADOS PESSOAIS

Tribunal Constitucional Espanhol

Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Informações básicas:
http://elpais.com/diario/2000/12/08/sociedad/976230015_850215.html

I. Antecedentes

1. Por escrito registrado en este Tribunal el 14 de marzo de 2000,el Defensor del Pueblo (art. 162 CE; art. 32 LOTC; arts. 5.4 y 29 de la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo), interpuso recurso de inconstitucionalidad contra incisos de los arts. 21.1 ("Comunicación de datos entre Administraciones Públicas") y 24.1 y 2 ("Otras excepciones a los derechos de los afectados") de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) por vulneración de los arts. 18.1 y 4 y 53.1 CE.

2. A juicio del Defensor del Pueblo los incisos recurridos de ambos preceptos lesionan el contenido esencial de los derechos fundamentales del art. 18.1, en relación con lo dispuesto en su apartado 4, y la reserva de ley del art. 53.1 CE.

(...)

a) En lo que hace a la impugnación parcial del art. 21.1 LOPD, al regular la comunicación de datos entre Administraciones Públicas, en r elación con lo dispuesto en el art. 20.1 LOPD, aduce el Defensor del Pueblo en su recurso que la interpretación conjunta de los dos preceptos legales recurridos produce el resultado de que la LOPD posibilita, en primer lugar, que puedan hacerse cesiones de datos entre Administraciones Públicas para fines distintos a los que motivaron su recogida. En segundo lugar, que el titular de esos datos no sea informado, cuando se recaban, de la posibilidad de dicha cesión, al no estar prevista en la norma que crea y regula el fichero. En tercer lugar, que la propia cesión se efectúa sin el consentimiento del afectado. Y, en cuarto y último lugar, que la autorización para efectuar esas cesiones puede contenerse en una norma de rango inferior a la Ley.

(...)

Dice el Defensor del Pueblo que la facultad de consentir sobre la cesión de datos personales forma parte y es una garantía necesaria del derecho a la intimidad de su titular (arts. 4, 5 y 11 LOPD), pues sin esa facultad sería imposible controlar mínimamente la circulación de la información que las Administraciones hayan recabado sobre su persona, debilitando la protección que a dichos datos ofrece la propia Constitución.

(...)

5. El Abogado del Estado, en la representación que ostenta del Gobierno de la Nación, presentó su escrito de alegaciones en este Tribunal el 18 de abril de 2000.

(...)

En lo que hace a la impugnación del art. 24.1 LOPD (que guarda relación con los arts. 10 y 13.1 de la Directiva 95/46/CE) en sus incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas" y "la persecución de infracciones... administrativas", aduce el Abogado del Estado que dicho precepto excepciona lo previsto en los apartados 1 y 2 del art. 5 LOPD, que confiere a los individuos un derecho de información en la recogida de datos, pero lo hace de forma muy restringida. La Administración Pública puede negar ese derecho de información si al suministrarla impide o dificulta gravemente el ejercicio de las funciones de control y verificación, no bastando que simplemente genere dificultades en su desempeño. En opinión del Abogado del Estado la decisión legislativa de que tal derecho de creación legal deba ceder cuando su ejercicio conlleve la privación de efectividad de aquellas funciones administrativas o se dificulte su desempeño gravemente es perfectamente constitucional.

(...)

c) Para concluir su escrito de alegaciones, el Abogado del Estado aborda la impugnación del art. 24.2 LOPD. En dicho precepto se excepcionan los derechos de acceso, rectificación y cancelación de los datos personales establecidos en los arts. 15 y 16.1 LOPD, "si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección".

(...)

Para el Defensor del Pueblo, los derechos de los afectados a ser informados y a consentir así como los de acceso, rectificación y cancelación, integran el derecho fundamental de todos a controlar la recogida y el uso de aquellos datos personales que puedan poseer tanto el Estado y otros Entes públicos como los particulares. Lo que forma parte del contenido esencial (art. 53.1 CE) de los derechos fundamentales a la intimidad personal y familiar (art. 18.1 CE) y a la autodeterminación informativa (art. 18.4 CE). Por lo que cualquier restricción de aquellos derechos lo es de estos derechos fundamen-

tales y menoscaba su contenido esencial. Restricción que a juicio del Defensor del Pueblo se ha producido en la Ley impugnada por dos órdenes de razones.

(...)

Lo que debemos precisar es, pues, si el legislador ha vulnerado la reserva de ley (art. 53.1 CE), bien por renunciar a su regulación o por apoderar a la Administración para que restrinja tales derechos a su discreción. Pues es indudable que los arts. 21.1 y 24.1 y 2 LOPD han regulado el ejercicio de derechos de los individuos que forman parte del haz de facultades que integra el contenido del específico derecho fundamental a la protección de datos personales derivado de los arts. 18.1 y 18.4 CE, al que a continuación se hará referencia con mayor detenimiento.

(...)

4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.

(...)

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

(...)

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, s ino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

(...)

el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

(...)

De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), "se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección". De este modo, la LOPD puede ser contraria a la Constitución por vulnerar el derecho fundamental a la protección de datos (art.18.4 CE), por haber regulado el ejercicio del haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal prescindiendo de las precisiones y garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula (art. 53.1 CE).

(...)

Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen.

(...)

El motivo de la inconstitucionalidad del art. 21.1 LOPD resulta, pues, claro. La LOPD en este punto no ha fijado por sí misma, como le impone la

Constitución (art. 53.1 CE), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 LOPD, en relación con lo dispuesto en los arts. 4, 6 y 34.e LOPD), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar.

(...)

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.

(...)

FALLO

En atención a todo lo expuesto, el Tribunal Constitucional,

POR LA AUTORIDAD QUE LE CONFIERE LA CONSTITUCIÓN DE LA NACIÓN ESPAÑOLA,

Ha decidido

Estimar el presente recurso de inconstitucionalidad y, en consecuencia:

1º Declarar contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2º Declarar contrarios a la Constitución y nulos los incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1 del art. 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Publíquese esta Sentencia en el "Boletín Oficial del Estado".

Dada en Madrid, a treinta de noviembre de dos mil.

Ireland Data Protection Commissioner Report on Facebook

Informações básicas: http://www.bbc.co.uk/news/technology-16289426

Executive Summary

This is a report of an audit of Facebook-Ireland (FB-I) carried out by the Office of the Data Protection Commissioner of Ireland in the period October-December 2011. It builds on work carried out by other regulators, notably the Canadian Privacy Commissioner, the US Federal Trade Commission and the Nordic and German Data Protection Authorities. It includes consideration of a number of specific issues raised in complaints addressed to the Office by the "Europe-versus-Facebook" group, the Norwegian Consumer Council and by a number of individuals.

The audit was conducted with the full cooperation of FB — I. It found a positive approach and commitment on the part of FB-I to respecting the privacy rights of its users. Arising from the audit, FB-I has already committed to either implement, or to consider positively, further specific "best practice" improvements recommended by the audit team. A formal review of progress is planned in July 2012.

The audit was conducted by reference to the provisions of the Data Protection Acts, 1988 and 2003, which give effect to the European Union's Data Protection Directive 95/46/EC. Account was taken of guidance issued by the EU's Article 29 Working Party1. The audit team followed the standard audit methodology used by the Office2.

(…)

As a "data controller", FB-I has to comply with the obligations set out in the law. The report summarises the audit team's conclusions on how FB-I gives effect to the basic principles of data protection law: that personal data should be collected "fairly"; that the individual should be given comprehensive information on how personal data will be used by FB-I; that the personal data processed by FB-I should not be excessive; that personal data should be held securely and deleted when no longer required for a legitimate purpose; and that each individual should have the right to access all personal data held by FB-I subject to limited exemptions.

In addition to examining FB-I's practices under standard data protection headings, the team also examined in detail the data protection aspects of some specific aspects of FB-I's operations, such as its use of facial recognition technology for the "tagging" of individuals, the use of social plug-ins (the FB 'Like' button), the "Friends Finder" feature and the 3rd Party Applications ('Apps') operating on the FB platform.

In examining FB-I's practices and policies, it was necessary to examine its responsibilities in two distinct areas. The first is the extent to which it pro-

vides users with appropriate controls over the sharing of their information with other users and information on the use of such controls — including in relation to specific features such as "tagging". This also includes the rights of non-users whose personal data might be captured by FB-I. Various recommendations have been made for "best practice" improvements in this area.

The second main area where we examined FB-I's practices and policies related to the extent to which FB-I uses personal data of users to target advertising to them. FB-I provides a service that is free to the user. Its business model is based on charging advertisers to deliver advertisements which are targeted on the specific interests disclosed by users. This basic "deal" is acknowledged by the user when s/he signs up to FB-I and agrees to the Statement of Rights and Responsibilities and the related Data Use Policy.

A key focus of the audit was the extent to which the "deal" could reasonably be described as meeting the requirements of fair collection and processing under the Data Protection Acts. While acknowledging that this is a matter of judgment — ultimately by Irish and European Courts — the general conclusion was that targeting advertisements based on interests disclosed by user's in the 'profile' information they provide on FB was legitimate. We also concluded that, by extension, information positively provided by users through 'Like' buttons etc could legitimately be used as part of the basic "deal" entered into between the user and FB-I. The legitimacy of such use is, in all cases, predicated on users being made fully aware, through transparent notices, that their personal data would be used in this manner to target advertisements to them. And any further use of personal data should only be possible on the basis of clear user consent. Various recommendations have also been made for general "best practice" improvements in this area.

The privacy governance structure within FB-I was also examined. The comprehensive settlement reached by the Federal Trade Commission (FTC) with Facebook and announced on 29 November 2011 should ensure that Facebook will adopt a rigorous approach to privacy and data protection issues for the next 20 years. The focus of the audit was on the possible changes needed to strengthen the capacity of FB-I to ensure compliance with the specific requirements of Irish and EU data protection law.

Progress on implementing the specific recommendations contained in the Report will be reviewed in July 2012. This will be part of the Office's continuing engagement with FB-I.

(…)

The recommendations in the Report do not carry an implication that FB-I's current practices are not in compliance with Irish data protection law. Neither do they represent formal decisions of the Commissioner on the complaints submitted to him as the Audit was led by me under the Commissioner's authority.

--

List of Recommendations and Findings (*editado*)

ISSUE	Conclusion/Best Practice Recommendation	FB-I Response	Target Implementation Date
Privacy & Data Use Policy Complexity & accessibility of user controls	FB-I must work towards: • simpler explanations of its privacy policies • easier accessibility and prominence of these policies during registration and subsequently • an enhanced ability for users to make their own informed choices based on the available information	FB-I will work with the Office to achieve the objectives of simpler explanations of its Data Use Policy, identify a mechanism to provide users with a basis to exercise meaningful choice over how their personal data is used, easier accessibility and prominence of these policies during and subsequent to registration, including making use of test-groups of users and non-users as appropriate.	End Q1 2012 and routinely thereafter
Advertising **Use of user data**	There are limits to the extent to which user-generated personal data can be used for targeted advertising. Facebook must be transparent with users as to how they are targeted by advertisers	FB-I will clarify its data use policy to ensure full transparency.	By the end of Q1 2012
	FB-I should move the option to exercise control over social ads to the privacy settings from account settings to improve their accessibility. It should also improve user knowledge of the ability to block or control ads that they do not wish to see again	Agreed.	By the end of Q1 2012.

ISSUE	Conclusion/Best Practice Recommendation	FB-I Response	Target Implementation Date
Advertising Use of user data	If, FB-I in future, considers providing individuals' profile pictures and names to third parties for advertising purposes, users would have to provide their consent.	FB-I will enter into discussions with this Office in advance of any plans to introduce such functionality.	n/a
	The current policy of retaining ad-click data indefinitely is unacceptable.	FB-I will move immediately to a 2-year retention period which will be kept under review with a view to further reduction.	Review in July 2012
Retention of data	The information provided to users in relation to what happens to deleted or removed content, such as friend requests received, pokes, removed groups and tags, and deleted posts and messages should be improved.	FB-I will comply with this recommendation in an updated Data use Policy.	By the end of Q1 2012.
	User's should be provided with an ability to delete friend requests, pokes, tags, posts and messages and be able to in so far as is reasonably possible delete on a per item basis.	FB-I will phase in such transparency and control to users on a regular basis.	FB-I has agreed to begin working on the project during Q1 of 2012. FB-I has committed to showing demonstrable progress by our July 2012 review. This time-scale takes account of the size of the engineering task.

ISSUE	Conclusion/Best Practice Recommendation	FB-I Response	Target Implementation Date
Retention of data	Users must be provided with a means to exercise more control over their addition to Groups	FB-I has agreed that it will no longer be possible for a user to be recorded as being a member of a group without that user's consent. A user who receives an invitation to join a group will not be recorded as being a member until s/he visits the group and will be given an easy method of leaving the group	By the end of Q1 2012.
	Personal data collected must be deleted when the purpose for which it was collected has ceased	FB-I will comply with requirements in relation to retention where the company no longer has a need for the data in relation to the purposes for which it was provided or received. Specifically it will: 1. For people who are not Facebook users or who are Facebook users in a logged out state, FB-I will take two steps with respect to the data that it receives and records through social plugins within 10 days after such a person visits a website that contains a social plugin. First, FB-I will remove from social plugin impression logs the last octet of the IP address when this information is logged. Second, FB-I will delete from social plugin impression logs the browser cookie set when a person visits Facebook.com.	Immediate and ongoing, subject to any legal holds placed on the data by civil litigation or law enforcement. The continuing justification for these periods will be kept under continuous assessment and will be specifically re-assessed in our July 2012 review.

ISSUE	Conclusion/Best Practice Recommendation	FB-I Response	Target Implementation Date
Retention of data		2. For all people regardless of browser state (logged in, logged out, or non-Facebook users), FB-I will delete the information it	
Facial Recognition/Tag Suggest	FB-I should have handled the implementation of this feature in a more appropriate manner and we recommended that it take additional steps from a best practice perspective to ensure the consent collected from users for this feature can be relied upon	FB-I will provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings. FB-I will discuss with this Office any plans to extend tag suggest to allow suggestions beyond confirmed Friends in advance of doing so.	First week January 2012 at the latest
Deletion of Accounts	There must be a robust process in place to irrevocably delete user accounts and data upon request within 40 days of receipt of the request (not applicable to back-up data within this period.)	FB-I had already devoted a substantial amount of engineering resources to progressing account deletion to an acceptable level and is committed to working towards the objectives outlined by this Office.	Review in July 2012

ISSUE	Conclusion/Best Practice Recommendation	FB-I Response	Target Implementation Date
Tagging	There does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it.	FB-I will examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review	In advance of July 2012

Bibliografia Adicional

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

GRIMMELMANN, James. Saving Facebook. Iowa Law Review, Vol. 94, p. 1137, 2009. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262822

KLOEPFER, Michael. Informationszugangsfreiheit und Datenschutz: Zwei Säulen des Rechts der Informationsgesellschaft. DöV. V. 6, 2003.

LIMBERGER, Têmis. A informática e a proteção à intimidade. Revista da AJURIS. Porto Alegre, n. 80, p. 319-333, dez. 2000.

MAÑAS, José Luis Piñar. Proteccion de Datos: Origen, Situacion Actual y Retos de Futuro. Anais do Seminario de Derecho y Jurisprudencia. Madri, 2008. Disponível em: http://www.fcje.org.es/wp-content/uploads/file/jornada15/2_PINAR_1.pdf.

MOREIRA, Renato de Castro. O Direito à liberdade informática. Revista da AJURIS. Porto Alegre, p. 139-167, dez. 1999.

B) PRIVACIDADE E GRANDES EMPRESAS

Federal Trade Commission (USA)

DOCKET NO. C-4336
In the Matter of
GOOGLE INC.,
a corporation.
Informações básicas:
http://info.abril.com.br/noticias/mercado/google-fecha-acordo-com-a-justica-sobre-buzz-30032011-38.shl

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "respondent" shall mean Google, its successors and assigns, officers, agents, representatives, and employees. For the purpose of Parts I, II, and III of this order, "respondent" shall also mean Google acting directly or through any corporation, subsidiary, division, website, or other device.

(…)

4. "Google user" shall mean an identified individual from whom respondent has collected information for the purpose of providing access to respondent's products and services.

5. "Covered information" shall mean information respondent collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

(...)

I.

IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise

control over the collection, use, or disclosure of covered information. B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that respondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and

B. Obtain express affirmative consent from the Google user to such sharing.

III.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including: A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.

E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part III of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons conducting such Assessments and preparing such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part III of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

(...)

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements that describe the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, with all materials relied upon in making or disseminating such statements;

B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

D. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VIII.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

IX.

This order will terminate on October 13, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later;

(…)

By the Commission.

Donald S. Clark

Secretary

SEAL:

ISSUED: October 13, 2011

http://techatftc.wordpress.com/2012/08/09/google/

Tech@FTC
FTC Settles with Google over Cookie Control Override
Ed Felten

Today the FTC announced a settlement with Google, in which the company agreed to pay $22.5 Million to settle charges that it misled consumers about its use of tracking cookies on the Safari browser. The Complaint and Order, which were approved by the Commission, are the official statement of the FTC's position on the case. In this post I'll explain some of the technical background in more detail — speaking just for myself.

Google's DoubleClick ad network uses tracking cookies to record a history of a user's activities across different web sites. A DoubleClick tracking cookie looks like this:

id: c5bffdc4700000c||t=1343680985|et=730|cs=002213fd484b7cb9af91248086

Google also uses cookies to offer an opt-out. If a consumer clicks the opt--out button, Google creates an opt-out cookie, which clobbers any tracking cookie that was in place before. The opt-out cookie looks like this:

id: OPT_OUT

If you have the opt-out cookie, Google won't place a tracking cookie on your computer. On most browsers this all works as described.

But Apple's Safari browser — the default browser on Macs, iPhones, and iPads — puts more stringent limits on how sites can use cookies. In its default setting ("Block cookies: From third parties and advertisers") Safari blocks most cookies coming from third parties. Users can change this setting, but very few do change it, so from here on, let's assume that Safari is in its default configuration.

Safari allows a site to deposit a cookie onto your computer whenever at least one of the following things is true:

1. you are visiting the site directly — that is, it is the "first party" site whose URL appears in the browser's address bar, or
2. the site already has a cookie present in your browser, or
3. the site is responding to a form that you submitted.

One consequence of this design is that Google's opt-out cookie mechanism doesn't work for Safari users — Google's attempt to deliver the opt-out cookie will fail because none of the three conditions hold.

The FTC alleged that Google told Safari users that they didn't need to worry about the unavailability of opt-out, because Safari's cookie controls would provide the same protection as the opt-out.

Unfortunately, according to the FTC, this promise wasn't kept. Google ended up placing tracking cookies in many Safari users' browsers despite its promise to give those users the same treatment as opted-out users.

Google placed the tracking cookies in two different ways.

First, if you went to the doubleclick.net website, perhaps by typing in the URL but more likely by clicking an ad placed by DoubleClick, then you would be given a DoubleClick tracking cookie. Safari allowed this because it treated DoubleClick as playing a first-party role in this interaction — but no cookie would have been given to an opted-out user of another browser.

(An important detail here: Though people sometimes talk about "first--party cookies" versus "third-party cookies," there is nothing about the cookie itself that is marked as either first-party or third-party. Instead, first-party and third-party areroles that a site can play in a particular interaction — in the same way that "home team" is not a permanent attribute of a sports team but merely a role that the team might occupy in today's game. When somebody says "first-party cookie," you should read that as "cookie associated with a site that is playing a first-party role at the moment.")

The second way that Safari users got DoubleClick tracking cookies was more complicated — and this is the one that has gotten the most attention. This part of the story starts with Google wanting to put a "social advertising" cookie onto users' computers. "Social advertising" is a feature that lets you click a "+1" button on an ad you like — and then shows the same ad to your friends with an indication that you liked it. If implemented in a straightforward way, this wouldn't work on Safari because Safari would block the placement of Google's social advertising cookie.

So Google overrode Safari's cookie controls. They sent Safari a file that looked like this:

```
<html>
<head></head>
<body>
<form id="drt_form" method=post action="/pagead/drt/si?p=XXX&ut=
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXX">
</form>
    <script>
      document.getElementById('drt_form').submit();
    </script>
</body>
</html>
```

I recorded this file in mid-December, 2011. The line that starts with "document…." is Javascript code that told the browser that the user had submitted a form — even though the user had done no such thing. (The "form"

was invisible and had neither content nor a Submit button, so the user could not actually submit it.) Safari, believing that the user had chosen to submit a form, would then allow Google to put a DoubleClick cookie on the user's computer. This was allowed under condition number 3 above.

Once the first cookie was in place, Safari would then — according to condition number 2 above — allow Google to deliver additional cookies from doubleclick.net, including the DoubleClick tracking cookie. So the end result of Google's form submission was to put DoubleClick tracking cookies on Safari users' browsers, despite Google's alleged promise not to do so.

If you use Safari, you probably received a DoubleClick tracking cookie from Google during the relevant time period. As part of the settlement, Google agreed to destroy as many as possible of the DoubleClick tracking cookies placed on Safari users' computers during the relevant period. To its credit, Google started destroying those cookies early, without waiting for the settlement to be finalized, so virtually all of the relevant cookies should be gone by now.

Bibliografia Adicional

BOYD, Danah. MARWICK, Alice. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128

LEONARDI, Marcel. Tutela e privacidade na Internet. 1. ed. São Paulo: Saraiva, 2012.

NISSEMBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy. n. 17, 1998. Disponível em: http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf

CAPÍTULO 4 — INTERNET E INOVAÇÃO COMERCIAL

A) RESPONSABILIDADE DE INTERMEDIÁRIO

REsp 1107024 — Mercado Livre (STJ)

Informações básicas:
http://www.stj.jus.br/portal_stj/objeto/texto/impressao.wsp?tmp.estilo=&tmp.area=398&tmp.texto=104154

Superior Tribunal de Justiça
RECURSO ESPECIAL Nº 1.107.024 — DF (2008/0264348-2)
RELATÓRIO
MINISTRA MARIA ISABEL GALLOTTI (Relatora): Trata-se de recurso especial interposto contra acórdão do Tribunal de Justiça do Distrito Federal e dos Territórios cuja ementa foi lavrada nos seguintes termos: PROCESSO CIVIL E CONSUMIDOR — AÇÃO DE INDENIZAÇÃO — FRAUDE EM SISTEMA DE PAGAMENTOS REALIZADOS EM MEIOS ELETRÔNICOS — INTERNET — RESPONSABILIDADE CIVIL DO PRESTADOR DE SERVIÇOS — CONTRATO DE GESTÃO DE PAGAMENTOS — INTERMEDIAÇÃO DE TRANSAÇÕES — ILEGITIMIDADE PASSIVA — REJEIÇÃO — PRESENÇA DE EXCLUDENTE DE RESPONSABILIDADE — CULPA EXCLUSIVA DO CONSUMIDOR — RECURSO PROVIDO.

1. A divulgação de produtos em sítios eletrônicos mediante remuneração implica na figuração destes sítios como verdadeiros prestadores de serviços àqueles que ali divulgam seus produtos.

2. O contrato de gestão de pagamentos, onde o sítio eletrônico responsável pela divulgação de produtos visa garantir o adimplemento das obrigações criadas em possível contrato de compra e venda, caracteriza real intervenção no mencionado contrato e determina, portanto, a legitimidade passiva da empresa interventora para eventuais discussões acerca de vícios na garantia contratada.

3. Verifica-se a culpa exclusiva do consumidor, quando este, após ter acesso aos meios de ilidir seus próprios prejuízos não o faz, ainda que por mero desleixo.

4. O não atendimento, por parte do consumidor, dos procedimentos de execução do contrato exaustivamente apresentados e explicados pelo fornecedor implicam na exoneração da responsabilidade do fornecedor por culpa exclusiva do consumidor (CDC, artigo 14, §3º, ii).

5. APELO CONHECIDO. PRELIMINAR REJEITADA. PROVIDO O RECURSO.

Em suas razões, o recorrente aponta a violação dos arts. 535 do Código de Processo Civil; 6º, inciso III, 14, caput e § 1º, incisos I, II e III e 25 do Código de Defesa do Consumidor, assim como divergência jurisprudencial entre os entendimentos esposados pelo Tribunal de Justiça do Distrito Federal e dos Territórios e pelo Tribunal de Justiça do Estado do Rio Grande do Sul. Em síntese, sustenta que o acórdão é omisso no que toca à questão da "impossibilidade de se exonerar a indenização por parte do causador do prejuízo", argumentando que "ao afastar a regra contida no artigo 25 do Código de Defesa do Consumidor, o Tribunal a quo acaba por afastar a cogência da r. norma" (fls. 352-e/STJ). Alega, ainda, que "a própria ré ao tentar se eximir da responsabilidade sobre a fraude (...) não prova, contudo, que o produto posto à disposição dos vendedores não é suscetível a fraudes. Ao contrário, o que se depreende é que o sistema é um ambiente propício para que as fraudes aconteçam" (fls. 356-e/STJ).

Contrarrazões apresentadas às fls. 380/390, nas quais se alega o óbice da Súmula 7 e ausência de violação de lei ou divergência jurisprudencial.

É o relatório.

RECURSO ESPECIAL Nº 1.107.024 — DF (2008/0264348-2)

VOTO

MINISTRA MARIA ISABEL GALLOTTI (Relatora): O recurso merece prosperar. O art. 14, do CDC, invocado como violado no recurso especial, está devidamente prequestionado no acórdão recorrido. Também está suficientemente demonstrada a divergência entre o acórdão recorrido e acórdão do Tribunal de Justiça do Rio Grande do Sul, que apreciou questão semelhante, a saber, fraude em transação feita por intermédio do Mercado Livre, mediante envio de e-mail falso ao vendedor, induzindo-o a remeter a mercadoria.

De início, observo que não assiste razão ao recorrente em relação à alegada violação ao art. 535, II, do Código de Processo Civil, pois não verifico, no caso dos autos, omissão ou ausência de fundamentação na apreciação das questões suscitadas.

Nesse passo, é de se ter presente que não está o órgão julgador obrigado a se pronunciar sobre todos os argumentos apontados pelas partes, a fim de expressar o seu convencimento. O pronunciamento acerca dos fatos controvertidos, a que está o magistrado obrigado, encontra-se objetivamente fixado nas razões do acórdão recorrido.

Quanto ao mérito, todavia, assiste razão ao recorrente, pois a moldura fático-probatória apresentada não conduz à conclusão no sentido da culpa exclusiva da vítima, conforme acenou o julgado impugnado.

Com efeito, a partir do exame da prova produzida, o juiz sentenciante observou que "o Mercado Livre envia mensagens eletrônicas muito semelhantes àquela recebida pelo autor, comunicando a venda ou a compra de itens levados ao leilão eletrônico" e que, "ao fazer uso do 'e-mail', o Mercado Livre possibilita que estes sejam falsificados ou fraudados, considerando que os procedimentos de segurança são insuficientes", para, ao final, inferir que "não há preocupação do réu com a segurança ou combate à fraude, do que resulta na imputação de responsabilidade objetiva, decorrente do risco produzido a partir das suas atividades lucrativas de intermediação de compra e venda" (fls. 220-e/STJ).

O acórdão ora recorrido, por sua vez, após detalhar o mecanismo de intermediação disponibilizado pelo recorrido, consignou que "no caso em apreço ocorreu uma fraude em tal sistema de pagamentos. O fraudador mencionou interesse em adquirir o produto e, pouco após, fazendo-se passar pela instituição intermediadora, o próprio fraudador, utilizando-se de correio eletrônico da instituição intermediadora, enviou correio eletrônico ao vendedor informando falsamente que o valor referente à compra do bem já se encontrava à disposição, e que o bem já poderia ser enviado ao comprador" (fls. 319-e/STJ), concluindo pela culpa exclusiva do consumidor que, "seja por desleixo ou por pressa em realizar o contrato, não seguiu fielmente o procedimento apresentado, enviando o produto ao fraudador sem antes realizar a confirmação prévia do depósito junto à instituição intermediadora" (fls. 322/e-STJ).

Diante dessas informações, verifico que a hipótese dos autos não descreve uma situação de culpa exclusiva do consumidor. O autor aderiu ao contrato de gestão de pagamento mantido pelo réu (Mercado Pago) exatamente em função da segurança no recebimento dos valores que o sistema alardeava proporcionar. Conforme consignado expressamente no acórdão recorrido, o contrato de gestão de pagamento mencionava tão somente que a empresa intermediadora se compromete a notificar a 'recepção dos valores ao Comprador e ao Vendedor dentro do prazo referido na página MercadoPago no site'; a informação acerca da confirmação do pagamento encontrava-se veiculada no sítio eletrônico da empresa ré e, no entender do acórdão, "apesar de não integrar o contrato, deveria ter sido observada pelo autor porque assim refletiria a sua verdadeira atuação de boa-fé." (e-STJ, fl. 322).

É verdade que o autor não seguiu rigorosamente o procedimento sugerido no site quanto à confirmação do depósito, mediante verificação na conta respectiva constante em página do site, antes de enviar o produto. Mas, por outro lado, igualmente é certo que tal exigência de confirmação da veracidade do e-mail recebido em nome do site não constava do contrato de adesão. Igualmente não há dúvida de que o sistema de intermediação não ofereceu a segurança que legitimamente dele se esperava, dando margem à fraude. De fato, se, nos termos da sentença de mérito, o próprio "Mercado Livre envia

mensagens eletrônicas muito semelhantes àquela recebida pelo autor, comunicando a venda ou a compra de itens levados ao leilão eletrônico", fato este incontroverso, o autor, ao enviar a mercadoria, agiu de boa-fé, certo de que o pagamento já estaria de posse do serviço de intermediação do negócio e de que lhe seria disponibilizado assim que o comprador acusasse o recebimento do produto vendido.

A providência, sugerida no site (mas não prevista no contrato de adesão, conforme consignado no acórdão recorrido), no sentido da conferência, pelo consumidor, da mensagem supostamente enviada em nome do site, configura medida de segurança útil apenas em casos em que há fraude, a qual não se presume, não sendo absolutamente necessária ao aperfeiçoamento do negócio. É medida exclusiva de segurança, que se consubstancia, na prática, na transferência para o consumidor de uma parcela significativa do ônus relativo à segurança do negócio, que, ainda que tolerável em alguns casos, não tem o condão de afastar a responsabilidade do fornecedor, especialmente no caso, em que a sua apuração é objetiva e a segurança se confunde com o próprio serviço, isto é, o produto denominado Mercado Pago — oferecido de forma onerosa pelo Mercado Livre — é um serviço de mediação segura das contratações eletrônicas de compra e venda operadas por meio do sítio eletrônico. O objetivo da contratação do serviço de intermediação é exatamente proporcionar segurança ao comprador e ao vendedor quanto ao recebimento da prestação contratada.

Sob essa perspectiva, o descumprimento, pelo consumidor, da aludida providência, a qual sequer consta do contrato de adesão — a conferência da lisura e autenticidade da mensagem recebida —, não é suficiente para eximir o recorrido da responsabilidade pela segurança do sistema por ele implementado, sob pena de transferência ilegal de um ônus próprio da atividade empresarial por ele explorada. Trata-se, portanto, de estipulação de cláusula exoneratória ou atenuante de responsabilidade, terminantemente vedada pelo Código de Defesa do Consumidor (art. 25).

É de se ter presente, a propósito, que, em casos tais, o endereço eletrônico do vendedor é fornecido ao fraudador pelo próprio Mercado Livre, pois, como é sabido, os dados pessoais das partes, nessa modalidade de negociação, somente são revelados ao comprador após a sua aceitação à proposta de venda. Ou, em outros termos: somente após o fraudador — que obrigatoriamente fez sua regular inscrição no sítio e obteve a sua senha eletrônica — ter efetivado a compra do produto anunciado, via sistema eletrônico, é que o endereço eletrônico do vendedor foi disponibilizado pelo sistema.

Nesse aspecto impressiona também o fato de que o Mercado Livre tenha optado por apenas contestar a sua responsabilidade, alegando, inclusive, a sua ilegitimidade passiva, mas, no entanto, não tenha cuidado de identificar o suposto fraudador ou mesmo de chamá-lo ao processo, uma vez que é o

único detentor do cadastro e, portanto, dos dados utilizados pelo criminoso. Obviamente, não obstante, se os dados cadastrais utilizados pelo estelionatário também são falsos, revela-se certa fragilidade do sistema eletrônico utilizado pelo Mercado Livre, que permite a entrada de pessoas inescrupulosas na comunidade de usuários.

Sob esse prisma, entendo que a fraude foi iniciada com a livre entrada do invasor no sistema, franqueada pela deficiência do sistema cadastral, aperfeiçoando-se, no entanto, somente após o envio, pelo vendedor, do produto anunciado. Manifesto, portanto, o nexo causal entre o dano e a falha de segurança do serviço oferecido pelo recorrido.

De se notar, ainda, que o sistema eletrônico desenvolvido pelo Mercado Livre explora mercado novo, com o uso de novas tecnologias, dentro de um ambiente também novo, virtual, cujas especificidades ainda podem não ser amplamente dominadas pelo homem médio.

Isso significa, na prática, que muitos dos usuários tomam conhecimento do conteúdo do site, mas nem sempre são capazes de decifrá-lo completamente ou de operar, imediatamente, com segurança e desenvoltura as ferramentas colocadas à sua disposição. Não é, pois, razoável exigir que todos os usuários estejam perfeitamente adaptados, de pronto, às particularidades do sistema de dados desenvolvido pelo fornecedor. Não se justifica, pois, que procedimentos fundamentais à segurança de sistema de mediação eletrônica de pagamentos explorado por empresa comercial sejam atribuídos à responsabilidade exclusiva do usuário do serviço. A ausência de mecanismo de autenticação digital de mensagens, consentâneo com as exigências das modernas atividades empresariais que se desenvolvem no ambiente virtual, configura grave falha de segurança, que não deve ser imputada ou suportada pelo consumidor, mas pela empresa que assume o risco da atividade econômica.

O entendimento ora esposado está na linha do decidido pela 2ª Seção, a propósito da responsabilidade civil objetiva de instituições financeiras por danos causados por fraudes e delitos praticados por terceiros. Ficou estabelecido, "para os efeitos do art. 543-C, do CPC, que "as instituições bancárias respondem objetivamente pelos danos causados por fraudes ou delitos praticados por terceiros — como, por exemplo, abertura de conta-corrente ou recebimento de empréstimos mediante fraude ou utilização de documentos falsos —, porquanto tal responsabilidade decorre do risco do empreendimento, caracterizando-se como fortuito interno." (REsp. 1.199.782-PR, rel. Ministro Luis Felipe Salomão, DJe 12.9.2011).

Em face do exposto, dou provimento ao recurso especial, para restabelecer a sentença de mérito.

É como voto.

Bibliografia Adicional

MIRAGEM, Bruno. Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. Revista de Direito do Consumidor. N. 70. p. 41. São Paulo: Revista dos Tribunais, 2009.

LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. 1. ed. São Paulo: Juarez de Oliveira, 2005.

FINKELSTEIN, M. E.. Direito do Comércio Eletrônico. 2a.. ed. Rio de Janeiro: Ed. Campus Elsevier, 2010.

SILVA JUNIOR, Ronaldo Lemos da ; SOUZA, Carlos Affonso Pereira de ; BRANCO, Sergio. 'Responsabilidade Civil da Internet: uma breve reflexão sobre a experiência brasileira e norte-americana'. Revista de Direito das Comunicações, v. 1, p. 80-98, 2010.

B) MODELOS DE DISTRIBUIÇÃO DE CONTEÚDO — O CASO DO REDIGI

http://www.wired.com/threatlevel/2012/02/pre-owned-music-lawsuit-2/

Judge Refuses to Shut Down Online Market for Used MP3s

David Kravets
February 2nd, 2012

A one-of-a-kind website enabling the online sale of pre-owned digital--music files got a legal boost late Monday when a federal judge refused to shutter it at the request of Capitol Records.

It could be short-lived boost, however.

ReDigi, which opened in October, says it's a modern-day, used-record store that provides account holders with a platform to buy and sell used MP3s that were purchased lawfully through iTunes. The platform's technology does not support other digital files such as those purchased from Amazon or ripped from a CD.

The brief ruling (.pdf) by U.S. District Judge Richard Sullivan of New York did not clearly outline the reason for the decision. But in a transcript (.pdf) of a court proceeding Monday, he said that Capitol is likely to prevail at trial.

"I think (the) liklihood of success on the merits is something that plaintiffs have demonstrated," Judge Sullivan said from the bench.

Among others, the legal questions before the judge included the first-sale doctrine, the legal theory that people in lawful possession of copyrighted material have the right to sell it.

Sullivan's decision means that the case is still headed to trial, where Capitol will attempt to prove its allegations that ReDigi facilitates wanton copyright infringement and is not protected by the first-sale doctrine.

John Ossenmacher, ReDigi's founder, blasted Capitol in a statement. "We hope Capitol can get back to their business and find a way to catch up to the times instead of trying to stop the innovation process, denying rights to their paying customers along the way," he said.

Richard Mandel, Capitol's attorney, said in a telephone interview that "We are confident we will prevail at trial."

A different federal judge sided with the first-sale principle in 2008, when it debunked UMG Recordings' claim that it retained perpetual ownership of promotional CDs it releases before an album's debut. Last year, however, a different court ruled against now-defunct online service Zediva, which streamed movies to customers via DVDs that Zediva had purchased.

In the ReDigi case, Capitol Records sued the Massachusetts-based startup last month in New York federal court. Claiming ReDigi was not the used record store as it said it was, Capitol said ReDigi was liable for contributing to copyright infringement.

The label was demanding U.S. District Judge Richard Sullivan immediately order ReDigi to remove Capitol-owned material, (.pdf) and to also award damages of up to $150,000 per track against the startup. ReDigi would have gone defunct had the judge sided with Capitol.

ReDigi explained to Sullivan in court papers (.pdf) that its undisclosed number of account holders have a right to upload their purchased iTunes files into ReDigi's cloud. And when a file is sold to another ReDigi account holder, no copy is made. What's more, because of ReDigi's technology, the original uploaded file that is sold cannot be accessed by the seller any more through ReDigi or via the seller's iTunes account.

Prices for songs vary on ReDigi, with some files having asking prices as high as 87 cents — just 12 cents less than what many songs retail for on iTunes. The company, which earns up to 15 percent per sale, also offers cloud--storage music streaming.

—

http://www.innovationfiles.org/capitol-records-v-redigi-and-selling-used-digital-goods/

Capitol Records v. ReDigi and Selling "Used" Digital Goods

Daniel Castro
April 4, 2013

I recently wrote about the potential impact on differential pricing caused by the Supreme Court decision in Kirtsaeng v. John Wiley and Sons which found that the first sale doctrine applies to copyrighted works lawfully made abroad. I noted in that article that since most digital goods are licensed, not sold, differential pricing is still possible for digital goods, but that licensing has had side effects, such as limiting the ability of consumers to resell their digital goods in the used goods market.

Generally, consumers are allowed to legally buy and sell used goods. For example, if you buy a music CD, you can listen to it as many times as you want and then, if you don't plan to listen to it again and you haven't made any copies, legally sell the CD. But the same isn't true of digital goods that the consumer does not own but instead has only received a licensed to use.

For example, Amazon's MP3 store license agreement includes the following restrictions:

"You must comply with all applicable copyright and other laws in your use of the Music Content. Except as set forth in Section 2.1 above, you may not redistribute, transmit, assign, sell, broadcast, rent, share, lend, modify, adapt, edit, license or otherwise transfer or use the Music Content. We do not grant you any synchronization, public performance, promotional use, commercial sale, resale, reproduction or distribution rights for the Music Content. As required by our Music Content providers, Music Content is available only to customers located in the United States."

Recently, one company has attempted to change this. ReDigi has tried to create a virtual marketplace for "pre-owned" digital music so that individuals can legally buy and sell songs. Their basic idea is to have a three step process:

1.Users install ReDigi's software which identifies if certain digital music files are legally owned.

2.Users upload music they legally own to ReDigi's cloud storage service.

3.Users offer this music for sale. If someone buys a particular song, the seller loses access to that file and the buyer gains access. No new copies of the file are made — changes are only made to cloud-based access control system.

ReDigi argues that step two is legal because users are allowed to backup copies of their files under fair use and step three is legal because they are not creating any copies of the files (again, only changing the access control permissions). Not surprisingly, some rights holders are skeptical of the ReDigi system and have challenged its legality.

This past week a U.S. District Court issued a ruling in Capitol Records, LLC. v. ReDigi Inc. that rejected ReDigi's arguments. The court found that while copying music files to a cloud service does not necessarily violate fair use, copying these files to a cloud service for the purpose of selling the music does fall outside of fair use. In addition, since the court does not believe the copy falls under fair use, it is not a lawful copy and therefore not subject to the first sale doctrine.

The court is quite explicit in its ruling:

"Here, a ReDigi user owns the phonorecord that was created when she purchased and downloaded a song from iTunes to her hard disk. But to sell that song on ReDigi, she must produce a new phonorecord on the ReDigi server. Because it is therefore impossible for the user to sell her "particular" phonorecord on ReDigi, the first sale statute cannot provide a defense. Put another way, the first sale defense is limited to material items, like records, that the copyright owner put into the stream of commerce. Here, ReDigi is not distributing such material items; rather, it is distributing reproductions of the copyrighted code embedded in new material objects, namely, the ReDigi server in Arizona and its users' hard drives. The first sale defense does

not cover this any more than it covered the sale of cassette recordings of vinyl records in a bygone era." (emphasis in original)

The ruling goes on to argue that U.S. copyright law quite clearly does not allow for secondary markets of "pre-owned" digital goods. Indeed, Reps. Boucher and Campbell had proposed legislation in 1997 to update Section 109 of the Copyright Act so that the first sale doctrine would apply to digital works, but their legislation was never enacted.

Of course, there are many reasons why not allowing users to sell "used" digital goods makes sense. As explained back in 2001 by Marybeth Peters, former Register of Copyrights:

"Physical copies degrade with time and use; digital information does not. Works in digital format can be reproduced flawlessly, and disseminated to nearly any point on the globe instantly and at negligible cost. Digital transmissions can adversely affect the market for the original to a much greater degree than transfers of physical copies."

But while digital goods may be intrinsically different than non-digital goods, should that necessarily exclude them from being re-sold? Back in 2001, Ms. Peters argued that the status of the technology necessary to allow the sale of used digital goods is uncertain. She wrote:

"Additionally, unless a 'forward-and-delete' technology is employed to automatically delete the sender's copy, the deletion of a work requires an additional affirmative act on the part of the sender subsequent to the transmission. This act is difficult to prove or disprove, as is a person's claim to have transmitted only a single copy, thereby raising complex evidentiary concerns. There were conflicting views on whether effective forward and delete technologies exist today. Even if they do, it is not clear that the market will bear the cost of an expensive technological measure."

Whether a system like ReDigi actually prevents music piracy is an open question. There is certainly a degree of consumer trust involved — and I'm sure it is possible to circumvent the system, at least on a limited basis. But the same is true when buying and selling CDs since it is impossible to be sure that the seller has not made an illegal copy. To its credit, ReDigi has implemented various controls to try to prevent users from cheating and keeping copies of the music that they upload. (For the full details, check out their FAQ "Is ReDigi Legal?")

There are no obvious answers here, but if Congress does consider additional reforms to the Copyright Act, it is worth revisiting whether the technology has changed enough to warrant rethinking the First Sale doctrine for digital goods or if we are willing to accept that the First Sale doctrine is no longer feasible in a digital world.

Bibliografia Adicional

Decisão Capitol Records v. ReDigi:
http://www.wired.com/images_blogs/threatlevel/2012/02/redigiruling1.pdf

LESSIG, Lawrence. The New Chicago School. The Journal of Legal Studies, n. 27, 1998.

GASSER, Urs. PALFREY Jr., John G. Catch-As-Catch-Can: A Case Note on Grokster. Research Publication No. 2005 — October 2005. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=869030.

C) SEARCH ENGINE NEUTRALITY

http://www.estadao.com.br/noticias/impresso,buscape-acusa-google-de-prejudicar-concorrentes,1082623,0.htm

Buscapé acusa Google de prejudicar concorrentes

Presidente da empresa de comparação de preços afirma que buscador beneficia os próprios produtos nos resultados

06 de outubro de 2013

RENATO CRUZ — O Estado de S.Paulo

Romero Rodrigues, presidente do Buscapé, resolveu aproveitar a discussão levantada pelo projeto de lei do Marco Civil da Internet para retomar sua reclamação contra o Google. Ele acusa o gigante americano da internet de beneficiar os próprios produtos (como o Google Shopping, concorrente do Buscapé) nos resultados das buscas, em detrimento dos produtos de outras empresas.

Em 2011, o Buscapé fez uma reclamação contra o Google ao Conselho Administrativo de Defesa Econômica (Cade). Até agora, não resultou em processo. O projeto do Marco Civil, que tramita no Congresso em regime de urgência, inclui o conceito de neutralidade de rede, que obriga as operadoras de telecomunicações a tratar de forma isonômica qualquer conteúdo que trafegue na internet.

De forma análoga, Rodrigues defende a neutralidade de busca, em que todo conteúdo deveria ser tratado da mesma forma pelo buscador. A seguir, os principais trechos da entrevista.

Qual é a importância da neutralidade de rede?

Uma das grandes discussões do Marco Civil está relacionada ao poder do consumidor. Se as telcos (operadoras de telecomunicações) puderem controlar a qualidade de serviço do site A ou do site B, na verdade estarão criando um padrão deturpado de navegação para o usuário, e pode ser criada uma situação de mercado em que não há isonomia, não há equilíbrio.

E o que isso tem a ver com buscadores?

Embaixo das telcos, ou em cima das telcos, existem os softwares de navegação e, acoplados aos softwares de navegação, existem os sites de busca. É muito perigoso discutir só neutralidade de rede sem discutir algo que hoje é muito debatido nos Estados Unidos, que é a neutralidade de busca. Porque, se você tem neutralidade de rede, mas não tem neutralidade de busca, o cenário final pode ser ainda pior do que se não houvesse neutralidade de rede. Sem neutralidade de rede, existem dois agentes de muito poder: a telco e o site de busca. No caso de existir neutralidade de rede, mas não a de busca, o site de busca se

torna ainda mais poderoso. O mundo todo está discutindo a discriminação de sites de buscas monopolistas a competidores verticais de seus produtos.

Como essa situação afeta vocês hoje?

É uma situação delicada, difícil. Ela se agrava todo dia porque, obviamente, a dependência é muito grande. Hoje o número de pessoas que digitam "www.buscape.com.br" é muito menor do que aquelas que digitam na barra de ferramenta de navegação simplesmente "buscapé" e clicam no primeiro resultado de busca. Todos hoje são obrigados a comprar o primeiro resultado de busca, porque alguns players de busca não reconhecem leis de marcas, de propriedade intelectual. Eles dizem que o seu competidor pode comprar (como publicidade) a sua palavra-chave (a própria marca), e então você tem de, na verdade, comprar a sua palavra-chave, para se defender desse movimento. O usuário acaba sendo pedagiado.

Mas o Marco Civil não teria impacto nessa área...

Hoje ele não cita nada sobre isso, mas eu acho um tema relevante, porque, num curto prazo, isso traz uma degradação do serviço ao consumidor. Ele vai pagar mais pela mesma coisa ou mais, às vezes, até por menos. Nos Estados Unidos, o principal site de busca também tem um serviço de shopping. O serviço foi gratuito durante dez anos, e isso enfraqueceu muito os comparadores de preço. Agora que outros comparadores de preço praticamente já não existem, o serviço passou a ser pago. E não só é pago, como é mesclado ao próprio serviço de anunciar no site de busca, o que tem feito aumentar muito o preço dos anúncios nos Estados Unidos. E esse preço o varejo está repassando para quem? Para o consumidor. Então, toda vez que você tem menos opções em qualquer tipo de mercado e de setor, você tem um repasse de preço para o consumidor.

Essa situação afeta outras empresas?

O longo prazo é mais preocupante. Além do Buscapé, eu sou investidor-anjo (investidor em empresas iniciantes). Eu converso com startups. Hoje a pergunta mais importante que qualquer startup tem de saber responder é: se o principal player de busca entrar no seu setor, como você faz para ele não te matar rápido? Então, quando um player consegue controlar o destino do tráfego, isso coloca em risco a criação de novos modelos de negócios. Passa a ser necessário criar negócios que não dependam dele, que não tenham interfaces com ele. Aí acabam surgindo apenas modelos de negócios acessórios, marginais, com características superlocais, ou que têm de entregar caixas ou qualquer coisa que não tenha um componente digital muito grande.

Como o sr. avalia o buscador de preços do Google?

Foi lançado há dois anos, quando fizemos o nosso pedido ao Cade. Acho que a principal questão não é nem o produto. Acho que tanto o Buscapé quanto os concorrentes do Buscapé têm capacidade de desenvolver produtos de uma forma muito interessante. Tanto que hoje raramente o consumidor encontra os preços mais baixos no shopping do buscador. O problema é que, quando

você faz a busca de um produto, o serviço de busca discrimina todos os outros comparadores, colocando o comparador do próprio serviço em pura iminência. Seria como se a Net lançasse um canal de compras e colocasse o canal não só na primeira posição, no canal 1, como no 18 (Globo em São Paulo), como no canal em que se liga a TV, e também onde era o meu canal e me jogasse mais para baixo, lá no canal seiscentos e tanto. Esse é o grande problema.

E qual seria a solução?

A solução que se dá para isso é deixar bem claro e bem separado um produto do outro. Por que o shopping desse buscador pega carona tão forte no outro serviço e não compete simplesmente nas mesmas regras? Ter uma aba escrita shopping é ok. Fazer propaganda na TV ou em qualquer lugar é ok. Mas por que aparecer sempre na primeira posição do resultado do Google, com direito a fotografia, com direito a vários links, com muito mais espaço, enquanto os outros ficam abaixo?

Essa situação tem prejudicado o resultado de vocês?

Temos alguns dados e estamos acompanhando essa situação. Sim, teve impacto em audiência. Também registramos um aumento do preço para a compra de mídia na própria ferramenta de busca. Porque não existe uma transparência na compra e o preço depende de um índice de qualidade confidencial da ferramenta de busca. Esse índice vem caindo com o tempo, e faz com que tenhamos de pagar mais caro. Mas o que eu posso dizer em relação a isso é que estamos obviamente fornecendo ao Cade os números que temos, e nada além disso.

O sr. não pode revelar alguns desses números?

Não, estão em caráter de confidencialidade hoje.

Bibliografia Adicional

GRIMMELMANN, James. Some Skepticism About Search Neutrality. THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET, p. 435, Berin Szoka & Adam Marcus, eds., TechFreedom, January 2011. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1742444

INTRONA, Lucas D. NISSENBAUM, Helen. Shaping The Web: Why The Politics Of Search Engines Matters. Information Society, Vol. 16, No. 3. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222009

PASQUALE III, Frank. BRACHA, Oren. Federal Search Commission? Access, Fairness and Accountability in the Law of Search. Cornell Law Review, September 2008. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002453

CAPÍTULO 5 — DIREITOS AUTORAIS

A) COMO PROTEGER DIREITOS AUTORAIS?

Caso Scarlet Extended SA vs SABAM, Tribunal de Justiça da União Européia (C-70/70)

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Terceira Secção)
24 de Novembro de 2011
Informações básicas: https://www.laquadrature.net/en/eu-court-of-justice-censorship-in-name-of-copyright-violates-fundamental-rights

«Sociedade da informação — Direitos de autor — Internet — Software 'peer-to-peer' — Fornecedores de acesso à Internet — Instalação de um sistema de filtragem das comunicações electrónicas para impedir o intercâmbio de ficheiros que violem direitos de autor — Inexistência de obrigação geral de vigilância sobre as informações transmitidas»

(...)

2 Este pedido foi apresentado no âmbito de um litígio que opõe a Scarlet Extended SA (a seguir «Scarlet») à Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (a seguir «SABAM») devido à recusa da Scarlet em instalar um sistema de filtragem das comunicações electrónicas através de softwares de intercâmbio de arquivos (designados «peer-to-peer»), para impedir o intercâmbio de ficheiros que violem direitos de autor.

Quadro jurídico

Direito da União

Directiva 2000/31

«(45) A delimitação da responsabilidade dos prestadores intermediários de serviços, fixada na presente directiva, não afecta a possibilidade de medidas inibitórias de diversa natureza. Essas medidas podem consistir, designadamente, em decisões judiciais ou administrativas que exijam a prevenção ou a cessação de uma eventual infracção, incluindo a remoção de informações ilegais, ou tornando impossível o acesso a estas.

[...]

(47) Os Estados-Membros só estão impedidos de impor uma obrigação de vigilância obrigatória dos prestadores de serviços em relação a obrigações de natureza geral. Esse impedimento não diz respeito a obrigações de vigilância

em casos específicos e, em especial, não afecta as decisões das autoridades nacionais nos termos das legislações nacionais.»

[...]»

5 Segundo o artigo 12.° da referida directiva, que faz parte da secção 4 do capítulo II deste, intitulada «Responsabilidade dos prestadores intermediários de serviços»

«1. No caso de prestações de um serviço da sociedade da informação que consista na transmissão, através de uma rede de comunicações, de informações prestadas pelo destinatário do serviço ou em facultar o acesso a uma rede de comunicações, os Estados-Membros velarão por que a responsabilidade do prestador não possa ser invocada no que respeita às informações transmitidas, desde que o prestador:

a) Não esteja na origem da transmissão;

b) Não seleccione o destinatário da transmissão; e

c) Não seleccione nem modifique as informações que são objecto da transmissão.

[...]

3. O disposto no presente artigo não afecta a possibilidade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infracção.»

6 Nos termos do artigo 15.° da Directiva 2000/31, que também faz parte da secção 4 do capítulo II desta directiva:

«1. Os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços mencionados nos artigos 12.°, 13.° e 14.°, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar activamente factos ou circunstâncias que indiciem ilicitudes.

2. Os Estados-Membros podem estabelecer a obrigação, relativamente aos prestadores de serviços da sociedade da informação, de que informem prontamente as autoridades públicas competentes sobre as actividades empreen-

didas ou informações ilícitas prestadas pelos autores aos destinatários dos serviços por eles prestados, bem como a obrigação de comunicar às autoridades competentes, a pedido destas, informações que permitam a identificação dos destinatários dos serviços com quem possuam acordos de armazenagem.»

Directiva 2001/29

7 Nos termos do décimo sexto e quinquagésimo nono considerandos da Directiva 2001/29:

[...]

(59) Nomeadamente no meio digital, os serviços de intermediários poderão ser cada vez mais utilizados por terceiros para a prática de violações. Esses intermediários encontram-se frequentemente em melhor posição para porem termo a tais actividades ilícitas. Por conseguinte, sem prejuízo de outras sanções e vias de recurso disponíveis, os titulares dos direitos deverão ter a possibilidade de solicitar uma injunção contra intermediários que veiculem numa rede actos de violação de terceiros contra obras ou outros materiais protegidos. Esta possibilidade deverá ser facultada mesmo nos casos em que os actos realizados pelos intermediários se encontrem isentos ao abrigo do artigo 5.° As condições e modalidades de tais injunções deverão ser regulamentadas nas legislações nacionais dos Estados-Membros.»

8 O artigo 8.° da Directiva 2001/29 dispõe:

«1. Os Estados-Membros devem prever as sanções e vias de recurso adequadas para as violações dos direitos e obrigações previstas na presente directiva e tomar todas as medidas necessárias para assegurar a aplicação efectiva de tais sanções e vias de recurso. As sanções previstas devem ser eficazes, proporcionadas e dissuasivas.

[...]

3. Os Estados-Membros deverão garantir que os titulares dos direitos possam solicitar uma injunção contra intermediários cujos serviços sejam utilizados por terceiros para violar um direito de autor ou direitos conexos.»

Directiva 2004/48

9 Segundo o vigésimo terceiro considerando da Directiva 2004/48:

«Sem prejuízo de outras medidas, procedimentos e recursos disponíveis, os titulares do direito deverão ter a possibilidade de requerer uma injunção contra um intermediário cujos serviços estejam a ser utilizados por terceiros para violar os direitos de propriedade industrial do titular. As condições e

regras relativas a tais injunções ficarão a cargo da legislação nacional dos Estados-Membros. No que diz respeito às violações de direitos de autor e direitos conexos, a Directiva [2001/29] já prevê um nível global de harmonização. Por conseguinte, o disposto no n.° 3 do artigo 8.° da Directiva [2001/29] não deve ser prejudicado pela presente directiva.»

(...)

11 O artigo 3.° da Directiva 2004/48 prevê:

«1. Os Estados-Membros devem estabelecer as medidas, procedimentos e recursos necessários para assegurar o respeito pelos direitos de propriedade intelectual abrangidos pela presente directiva. Essas medidas, procedimentos e recursos devem ser justos e equitativos, não devendo ser desnecessariamente complexos ou onerosos, comportar prazos que não sejam razoáveis ou implicar atrasos injustificados.

2. As medidas, procedimentos e recursos também devem ser eficazes, proporcionados e dissuasivos e aplicados de forma a evitar que se criem obstáculos ao comércio lícito e a prever salvaguardas contra os abusos.»

(...)

Litígio no processo principal e questões prejudiciais

15 A SABAM é uma sociedade de gestão que representa os autores, os compositores e os editores de obras musicais, autorizando a utilização das suas obras protegidas por terceiros.

16 A Scarlet é um fornecedor de acesso à Internet (a seguir «FAI») que proporciona aos seus clientes acesso à Internet, sem propor outros serviços como os de teledescarga ou de partilha de ficheiros.

17 Em 2004, a SABAM concluiu que os internautas que utilizam os serviços da Scarlet teledescarregam na Internet, sem autorização e sem pagar direitos, obras constantes do seu catálogo através de software «peer-to-peer», que é um meio transparente de partilha de conteúdos, independente, descentralizado e munido de funções de busca e de teledescarga avançadas.

18 Por acto de 24 de Junho de 2004, a SABAM citou a Scarlet perante o presidente do tribunal de première instance de Bruxelles, alegando que esta sociedade, enquanto FAI, era a melhor posicionada para tomar medidas destinadas a fazer cessar as violações dos direitos de autor cometidas pelos seus clientes.

19 Em primeiro lugar, a SABAM pediu que fosse declarada a existência de violações dos direitos de autor sobre as obras musicais pertencentes ao seu repertório, em particular do direito de reprodução e do direito de divulgação ao público, decorrentes do intercâmbio não autorizado de ficheiros electrónicos musicais realizado através de software «peer-to-peer», sendo essas violações cometidas mediante a utilização dos serviços da Scarlet.

20 Em seguida, pediu que a Scarlet fosse condenada a fazer cessar essas violações, sob pena de aplicação de uma sanção pecuniária compulsória, tornando impossível ou bloqueando qualquer forma de envio ou de recepção pelos seus clientes de ficheiros que contenham uma obra musical sem autorização dos titulares dos direitos, através de software «peer-to-peer». Por último, a SABAM pediu que a Scarlet lhe comunicasse, sob pena de aplicação de uma sanção pecuniária compulsória, uma descrição das medidas a aplicar para dar cumprimento à sentença que vier a ser proferida.

21 Por decisão de 26 de Novembro de 2004, o presidente do tribunal de première instance de Bruxelles declarou a existência da violação dos direitos de autor denunciada pela SABAM, mas, antes de decidir quanto ao pedido de cessação, nomeou um perito para avaliar se as soluções técnicas propostas pela SABAM eram tecnicamente exequíveis, se permitiam filtrar unicamente o intercâmbio ilícito de ficheiros electrónicos e se existiam outros dispositivos para controlar a utilização de software «peer-to-peer» e determinar os custos dos dispositivos previstos.

22 No seu relatório, o perito nomeado concluiu que, apesar de muitos obstáculos técnicos, não se pode excluir completamente que seja possível proceder a uma filtragem e a um bloqueio do intercâmbio ilícito de ficheiros electrónicos.

23 Por decisão de 29 de Junho de 2007, o presidente do tribunal de première instance de Bruxelles condenou a Scarlet a fazer cessar as violações dos direitos de autor declaradas na decisão de 26 de Novembro de 2004 tornando impossível qualquer forma de envio ou de recepção pelos seus clientes, através de software «peer-to-peer», de ficheiros electrónicos que contenham uma obra musical do repertório da SABAM, sob pena de aplicação de uma sanção pecuniária compulsória.

24 A Scarlet interpôs recurso dessa decisão para o órgão jurisdicional de reenvio alegando, em primeiro lugar, que lhe era impossível dar cumprimento à referida medida inibitória dado que a eficácia e a perenidade dos sistemas de bloqueio e de filtragem não estão demonstradas e que a instalação desses

dispositivos depara com numerosos obstáculos de ordem prática, como os problemas da capacidade da rede e do seu impacto na referida rede. Além disso, qualquer tentativa de bloqueio dos ficheiros em causa está votada ao insucesso a curto prazo, uma vez que actualmente existe software «peer-to-peer» que não permite a verificação do seu conteúdo por terceiros.

25 Em seguida, a Scarlet alegou que a referida medida inibitória não respeita o artigo 21.° da Lei de 11 de Março de 2003 relativa a determinados aspectos jurídicos dos serviços da sociedade da informação, que transpõe para o direito nacional o artigo 15.° da Directiva 2000/31, porque lhe impõe, de facto, uma obrigação geral de vigilância das comunicações na sua rede, na medida em que qualquer dispositivo de bloqueio ou de filtragem de tráfego «peer-to-peer» pressupõe necessariamente uma vigilância generalizada de todas as comunicações que passam por essa rede.

26 Por último, a Scarlet considerou que a instalação de um sistema de filtragem viola as disposições do direito da União sobre a protecção de dados pessoais e a confidencialidade das comunicações, uma vez que essa filtragem implica o processamento dos endereços IP, que são dados pessoais.

27 Neste contexto, o órgão jurisdicional de reenvio considerou que, antes de verificar se existe um mecanismo de filtragem e de bloqueio de ficheiros «peer-to-peer» e se esse mecanismo pode ser eficaz, se deve garantir que as obrigações susceptíveis de serem impostas à Scarlet estão em conformidade com o direito da União.

28 Nestas condições, a cour d'appel de Bruxelles decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1. As Directivas 2001/29/CE e 2004/48/CE, conjugadas com as Directivas 95/46, 2000/31 e 2002/58, interpretadas à luz dos artigos 8.° e 10.° da Convenção Europeia para a protecção dos Direitos do Homem e das liberdades fundamentais, permitem que os Estados-Membros confiram competência a um juiz nacional, [que conhece do mérito] de um processo [...] e com base numa única disposição legal que prevê que: '[o juiz nacional] pode igualmente dirigir uma injunção de cessação aos intermediários cujos serviços sejam utilizados por um terceiro para violar os direitos de autor ou um direito conexo', para ordenar a um fornecedor de acesso à Internet (abreviadamente «FAI») [a instalação], em relação a toda a sua clientela, em abstracto e a título preventivo, a expensas exclusivas desse FAI e sem limitação no tempo, de um sistema de filtragem de todas as comunicações electrónicas, tanto as que

entram como as que saem, transitando pelos seus serviços, nomeadamente através da utilização de software peer-to-peer, com vista a identificar na sua rede a circulação de ficheiros electrónicos contendo uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega possuir direitos, e bloquear de seguida a transferência desses ficheiros, seja no momento do pedido, seja no momento do envio?

2. Em caso de resposta afirmativa à primeira questão, essas directivas exigem que o juiz nacional, chamado a decidir sobre um pedido de injunção em relação a um intermediário cujos serviços são utilizados por um terceiro para violar os direitos de autor, aplique o princípio da proporcionalidade quando tiver de se pronunciar sobre a eficácia e o efeito dissuasor da medida requerida?»

Quanto às questões prejudiciais

29 Com as suas questões, o órgão jurisdicional de reenvio pergunta, no essencial, se as Directivas 2000/31, 2001/29, 2004/48, 95/46 e 2002/58, lidas conjuntamente e interpretadas à luz das exigências resultantes da protecção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que ordena a um FAI a instalação um sistema de filtragem

— de todas as comunicações electrónicas que transitam pelos seus serviços, nomeadamente através da utilização de software «peer-to-peer»;

— que se aplica indistintamente a toda a sua clientela;

— com carácter preventivo;

— exclusivamente a expensas suas; e

— sem limitação no tempo;

capaz de identificar na rede desse fornecedor a circulação de ficheiros electrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega ser titular de direitos de propriedade intelectual, com o objectivo de bloquear a transferência de ficheiros cujo intercâmbio viole direitos de autor (a seguir «sistema de filtragem controvertido»).

(...)

37 Nestas condições, há que analisar se a medida inibitória em causa no processo principal, que imporia ao FAI a instalação do sistema de filtragem

controvertido, o obrigaria, nessa ocasião, a proceder a uma vigilância activa da totalidade dos dados relativos a cada um dos seus clientes a fim de prevenir qualquer violação futura dos direitos de propriedade intelectual.

38 A este propósito, é pacífico que a instalação deste sistema filtragem implicaria

— em primeiro lugar, que o FAI identificasse, na totalidade das comunicações electrónicas de todos os clientes, os ficheiros que fazem parte do tráfego «peer-to-peer»;

— em segundo lugar, que identificasse, no quadro desse tráfego, os ficheiros que contêm obras sobre as quais os titulares dos direitos de propriedade intelectual alegam deter direitos;

— em terceiro lugar, que determinasse quais desses ficheiros eram trocados ilicitamente; e

— em quarto lugar, que procedesse ao bloqueio do intercâmbio de ficheiros que considerasse ilícito.

39 Deste modo, essa vigilância preventiva exigiria uma observação activa da totalidade das comunicações electrónicas efectuadas na rede do FAI em causa e, portanto, englobaria toda e qualquer informação a transmitir e todos os clientes que utilizam essa rede.

40 Em face do exposto, deve observar-se que a medida inibitória aplicada ao FAI em causa de instalar o sistema de filtragem controvertido o obrigaria a proceder a uma vigilância activa de todos os dados relativos aos seus clientes a fim de prevenir qualquer violação futura dos direitos de propriedade intelectual. Daqui se conclui que a referida medida inibitória imporia a esse FAI uma vigilância geral que é proibida pelo artigo 15.°, n.° 1, da Directiva 2000/31.

41 Para apreciar a conformidade dessa medida inibitória com o direito da União, há, além disso, que ter em conta as exigências resultantes da protecção dos direitos fundamentais aplicáveis, como os que são referidos pelo órgão jurisdicional de reenvio.

42 A este respeito, deve recordar-se que a medida inibitória em causa no processo principal tem por objectivo assegurar a protecção dos direitos de autor, que fazem parte do direito de propriedade intelectual, os quais são

susceptíveis de ser violados pela natureza e o pelo conteúdo de determinadas comunicações electrónicas efectuadas através da rede do FAI em causa.

43 É verdade que a protecção do direito de propriedade intelectual está consagrada no artigo 17.°, n.° 2, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»). Assim sendo, não decorre de forma alguma dessa disposição nem da jurisprudência do Tribunal de Justiça que esse direito seja intangível e que a sua protecção deva, portanto, ser assegurada de forma absoluta.

44 Com efeito, como decorre dos n.os 62 a 68 do acórdão de 29 de Janeiro de 2008, Promusicae (C-275/06, Colect., p. I-271), a protecção do direito fundamental de propriedade, em que se integram os direitos relacionados com a propriedade intelectual, deve ser ponderada conjuntamente com a de outros direitos fundamentais.

45 Em concreto, resulta do n.° 68 do referido acórdão que compete às autoridades e aos órgãos jurisdicionais nacionais, no âmbito das medidas adoptadas para proteger os titulares de direitos de autor, assegurar um justo equilíbrio entre a protecção deste direito e a dos direitos fundamentais das pessoas afectadas por essas medidas.

46 Assim, em circunstâncias como as do processo principal, as autoridades e os órgãos jurisdicionais nacionais devem, nomeadamente, assegurar um justo equilíbrio entre a protecção do direito de propriedade intelectual, de que gozam os titulares de direitos de autor, e a da liberdade de empresa de que beneficiam os operadores como os FAI nos termos do artigo 16.° da Carta.

47 Ora, no caso em apreço, a medida inibitória que ordena a instalação do sistema de filtragem controvertido implica a vigilância, no interesse dos referidos titulares, da totalidade das comunicações electrónicas efectuadas na rede do FAI em causa, sendo essa vigilância, além disso, ilimitada no tempo, visando qualquer violação futura e sendo suposto dever proteger não só as obras existentes mas também as obras futuras que ainda não foram criadas no momento da instalação do referido sistema.

48 Deste modo, a referida medida inibitória implicaria uma violação caracterizada da liberdade de empresa do FAI em causa, dado que o obrigaria a instalar um sistema informático complexo, oneroso, permanente e exclusivamente a expensas suas, o que de resto seria contrário às condições previstas no artigo 3.°, n.° 1, da Directiva 2004/48, que determina que as medidas

para assegurar o respeito dos direitos de propriedade intelectual não sejam desnecessariamente complexas ou onerosas.

49 Nestas condições, deve considerar-se que a medida inibitória que ordena a instalação do sistema de filtragem controvertido não respeita a exigência de assegurar um justo equilíbrio entre, por um lado, a protecção do direito de propriedade intelectual, de que gozam os titulares de direitos de autor, e, por outro, a da liberdade de empresa de que beneficiam os operadores como os FAI.

50 Acresce que os efeitos da referida medida inibitória não se limitariam ao FAI em causa, sendo o sistema de filtragem controvertido também susceptível de violar os direitos fundamentais dos clientes desse FAI, a saber, o seu direito à protecção dos dados pessoais, bem como a sua liberdade de receber ou de enviar informações, direitos que são protegidos pelos artigos 8.° e 11.° da Carta.

51 Com efeito, é ponto assente, por um lado, que a medida inibitória que ordena a instalação do sistema de filtragem controvertido implicaria uma análise sistemática de todos os conteúdos e a recolha e identificação dos endereços IP dos utilizadores que estão na origem do envio de conteúdos ilícitos na rede, sendo esses endereços dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores.

52 Por outro lado, a referida medida inibitória correria o risco de violar a liberdade de informação, dado que esse sistema poderia não distinguir suficientemente um conteúdo ilícito de um lícito, de modo que o seu accionamento poderia provocar o bloqueio de comunicações de conteúdo lícito. Com efeito, é pacífico que a resposta à questão da licitude de uma transmissão depende também da aplicação de excepções legais aos direitos de autor que variam de um Estado-Membro para outro. Além disso, em certos Estados-Membros, determinadas obras podem pertencer ao domínio público ou os autores em causa podem colocá-las gratuitamente à disposição do público na Internet.

53 Consequentemente, há que declarar que, ao adoptar a medida inibitória que obriga o FAI a instalar o sistema de filtragem controvertido, o órgão jurisdicional nacional não respeitaria a exigência de assegurar um justo equilíbrio entre o direito de propriedade intelectual, por um lado, e a liberdade de empresa, o direito à protecção dos dados pessoais e a liberdade de receber ou de enviar informações, por outro.

54 Em face do exposto, deve responder-se às questões submetidas que as Directivas 2000/31, 2001/29, 2004/48, 95/46 e 2002/58, lidas conjuntamente e interpretadas à luz das exigências resultantes da protecção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que ordena a um FAI a instalação do sistema de filtragem controvertido.

(...)

Pelos fundamentos expostos, o Tribunal de Justiça (Terceira Secção) declara:

As Directivas:

— 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»);

— 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação;

— 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de Abril de 2004, relativa ao respeito dos direitos de propriedade intelectual;

— 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados; e

— 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas);

lidas conjuntamente e interpretadas à luz das exigências resultantes da protecção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que ordena a um fornecedor de acesso à Internet a instalação de um sistema de filtragem

— de todas as comunicações electrónicas que transitam pelos seus serviços, nomeadamente através da utilização de software «peer-to-peer»;

— que se aplica indistintamente a toda a sua clientela;

— com carácter preventivo;

— exclusivamente a expensas suas; e

— sem limitação no tempo;

capaz de identificar na rede desse fornecedor a circulação de ficheiros electrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega ser titular de direitos de propriedade intelectual, com o objectivo de bloquear a transferência de ficheiros cujo intercâmbio viole direitos de autor.

Bibliografia Adicional

DALY, Angela. FARRAND, Benjamin. Scarlet v SABAM: Evidence of an Emerging Backlash Against Corporate Copyrights Lobbies in Europe? Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2095295

SOUZA, Carlos Affonso Pereira de. Compartilhamento, Colaboração e Pirataria: questionamentos atuais sobre direito autoral. Revista Forense (Impresso), v. 383, p. 31-46, 2006.

B) DIREITOS AUTORAIS E CROWDSOURCING

http://www.theverge.com/2012/5/7/3005044/roflcon-when-memes-go-mainstream (o texto é acompanhado de diversos vídeos curtos)

At ROFLCon, watching memes go mainstream

Reporting from ROFLCon III at MIT in Cambridge, Massachusetts, we find that not everything is LOL-worthy

I spent Friday and Saturday on the campus of MIT in Cambridge, Massachusetts attending ROFLCon III. What is ROFLCon? It's a biennial convention (this year was its third) held to celebrate and discuss internet memes and the celebrity that is often created alongside them. This year's invited guests included Chuck "Nope" Testa, Antoine Dodson, who became famous when he appeared on local news after a home invasion, Paul "Bear" Vasquez, AKA the "Double Rainbow" guy, and "Tron Guy" Jay Maynard. There are also internet celebs of a different ilk — people who have created loved and admired "works," like Chris Torres, creator of Nyan Cat, Matt Oswald, creator of the "Me Gusta" guy, or film editor Duncan Robson, creator of the very well known supercut "Let's Enhance." There were also academics, thinkers, and media on hand to round out the very diverse crew. Oh, and Scumbag Steve was there.

Like other conventions, ROFLCon is an assortment of prepared keynote speeches — this year's were by *I Can Has Cheezburger*'s CEO Ben Huh and Jonathan Zittrain, Professor of internet law at Harvard University, one-off presentations, and moderated panels on topics such as "Life After the Meme," and "Webcomics: The Longview."

Unlike a lot of other conventions, however, the atmosphere is laid back and mostly everyone seemed to be having a pretty great time. I'll admit, I wasn't sure what to expect (this was my first ROFLCon) going in, but the fairly joyful environment caught up with me. The discussions at ROFLCon covered a wide assortment of topics ranging from the funny to the very serious — things like intellectual property law, and data management for huge sites such as Reddit and YouTube — but for the most part, there was a prevailing vibe of positivity that I at first found to be endearing and hard to disagree with, but ultimately left feeling unsettled about.

Many of the people I spoke with at ROFLCon, or heard speak, echoed similar sentiments: while they didn't feel a direct sense of ownership over their creation, recognition is always nice. This was true of Paul Vasquez, whose "Double Rainbow" video first attracted attention when Jimmy Kimmel Twe-

eted it, but quickly went even more viral a few days later when it was turned into a song by AutoTune the news (the same thing happened to Antoine Dodson's home invasion news appearance). Paul, who maintains that he "saw God" when filming the rainbow, won't put ads on his YouTube video, and removes other videos he finds which are direct copies, but allows people to freely "remix" his video for other purposes.

Chris Torres, who created the Pop Tarted body with the head of a cat known as Nyan Cat, had a similar experience. After creating the cat, it was another person who set the animation to the Nyan song, creating a truly viral phenomenon which has inspired video games and hundreds of items in Etsy shops. Torres told me that he has his limits when it comes to the remix culture of Nyan Cat, however. For instance, he said, he wouldn't like to see representations of Nyan Cat being hurt (neither would I). There is, however, an overall sense that the creations are, to various extents, out of the creator's control once they hit the internet.

This is the essence of a meme, of course. The idea that an image or piece of video can be repeated, represented, played with and morphed over what is often a long period of time is central to a successful meme. Take for instance, "Success Kid." In 2007, Laney Griner uploaded a photo of her 11-month old baby Sammy on a beach eating sand, looking triumphantly at the camera, to her personal Flickr account. By early 2008, the image appeared on MySpace with the captions "Ima Fuck you up," and "I Hate Sandcastles." On stage at ROFLCon with Sammy, who is now nearly 5, Laney said she was at first confused. She didn't really know what memes were, and, she noted, Sammy loved sandcastles — he is, after all, eating sand in the photo. She wasn't pleased, at first, but Sammy really went viral when his photo began to appear with "advice animal" captions, befitting his victorious look in the photo. Captions like, "Put 5 dollars in pocket… pull out 10," and "Thought I only had one beer left… Two left" made Laney feel better, she said — once she "got it." Sammy's likeness was being used for something positive. The meme has generated hundreds of similarly captioned photos. The "Me Gusta" image, similarly, shows up ad nauseum in what are known as "rage comics," and creator Matt Oswald, who said it was drawn on a whim in 15 minutes before he uploaded it to 4Chan, says he doesn't even feel like he created it: the community, after all, gave it meaning, over months of repeating, morphing, and retelling. We can all agree that memes as we know them wouldn't be possible without the communities which create them through endless modification.

Another thing we can all agree on: memes and related internet culture are now mainstream. When ROFLCon started in 2008, memes were still for a niche (if very large) audience. There are great reasons for that. Memes don't explain themselves very well — you have to know how to read them, and you have to look at several examples before you "get" the joke.

The barrier to entry on "getting the joke" varies: the Chuck Testa "Nope" advertisement is pretty funny regardless of who you are and what you know about the internet, but you have to know the video before you can see why the related images of Chuck with the caption "Nope!" are funny. This is true of most memes, and a few years ago, most people simply weren't in on the joke. That is all changing very fast. Duncan Robson unveiled a new supercut, called "Three Point Landings" on Saturday, and the video already has nearly 100,000 views barely a day later. Nyan Cat makes an appearance in a Sprint 4G Nexus commercial entitled, "Cats," and Paul Vasquez and his Double Rainbow appeared in a Windows Live Photo Gallery commercial in 2010. Success Kid Sammy appeared on billboards in the UK for Virgin Media, as well as in a new Vitamin Water ad (Nyan Cat is in that one, too!). These companies are on the cutting edge of using the viral for advertisement, but they're also likely harbingers of where that advertising culture is going.

Of course, some people have managed to "profit," in more ways than one, from their often inadvertent brushes with celebrity. They get invited to ROFLCon, and they are genuinely adored by the people who attend. Some, such as Success Kid Sammy and his family, profit directly when they sell the rights to the image to Vitamin Water or Virgin Media. The Double Rainbow guy says he made enough money to "buy a used car" for his appearance in the Microsoft ad. Everyone at ROFLCon seemed to agree: good for them. But, at the same time, everyone also agreed that the continued right to remix those same images and videos should be a foregone conclusion. I won't argue with that one: supercut videos like Duncan Robson's excellent work simply couldn't exist without this freedom.

So what's the problem? Antoine Dodson possibly said it best when he famously told Good Morning America that he had a "hit on iTunes" but was still "in the projects" in 2010. Now, it's not like this guy wrote a great American novel, right? Right. The problem is that internet celebrities and memes are now making up a greater part of our "culture" than ever — and for some of us, they are almost the entirety of it. We consume them: we watch their videos millions of times, we caption their images freely and exuberantly, and the mainstream is waking up to that. But mainstream companies and their ad companies aren't playing for the same reasons — the mainstream is here to get paid. Many of the attendees whom I spoke to, once I talked to them long enough, mentioned that they weren't really better off financially than they had been before creating whatever they created, or becoming a meme, or finding their little corner of celebrity. The problem with this model is not that the subjects of our internet culture aren't profiting enough off of them: it's that literally everyone else is. The companies who make ads to sell their phones, the massive websites which post them and sell highly profitable ads against them, the makers who create Nyan Cat scarves. These are often highly successful ventures with massive corporate structures behind them.

Entire websites find their bread and butter in posting endless variations of Chuck Testa images, and it's not just highly criticized sites like I Can Has Cheezburger; even CNN routinely gets in on the game these days. Chuck himself, is in many ways, a cash cow for plenty of websites, but he's still running his taxidermy business, and told me flat out that he is "broke."

And, for what might be the first time, the creators of the content which we consume assert almost no right to it: they are happy, overjoyed, to be recognized and beloved. They're just pleased to be at ROFLCon. Some, like Paul Vasquez and Antoine Dodson, who unsurprisingly have big personalities to capitalize on, are trying to take their fame a bit further, to make an economic enterprise of it. Most, however, are not: they're regular people, or they're artists, or people with other, regular jobs, whose kids just happened to be so cute they became a phenomenon on YouTube. And, as I said, that's all well and good. The attendees at ROFLCon all agree, these people are treasures to a certain segment of the population. But increasingly, they are also a nearly endless fount of money-making possibilities, coming at little to no cost, with little to no gain for their subjects and creators.

It's probably unsurprising that this year was the last ROFLCon: the convention is being put on indefinite hiatus. Memes are now mainstream, not just for us weirdos at the far corners of the internet anymore. As we make ourselves comfortable with that joyful, open, and free reality, we should probably begin to rethink what "free" means, because someone, somewhere, is already trying to think of awesome new ways to capitalize on your accidental brush with memedom.

Meme Cuisine: Honey Badger Hot Sauce

BY JOSEPH FLAHERTY
08.24.12

Product licensing used to be so easy. If you wanted to make a Mickey Mouse watch, you'd ring up Walt Disney and negotiate terms. But what if you want to create products based on an internet meme like Philosoraptor or the honey badger? It's not like you can call 4chan to ask for permission.

However, that's just what Chris Glaister, Leigh Zalusky, and Paul Lees wanted to do. The trio of design engineers and amateur barbecue buffs decided to make a hot sauce based on the internet-famous critter. The team created a habanero-infused, "Cobra Strength," hot sauce and decided their creation required a container "vicious enough to contain this spicy awesomeness." So, they designed a custom bottle to honor the pugnacious mammal, and are now working on securing distribution.

In case you're unfamiliar with the meme, a narrator named "Randall" added a hilariously sassy voiceover to a National Geographic clip featuring a furry, fearless, cobra-killing creature called the honey badger. It became a YouTube sensation with 49 million views and counting.

While any redditor knows the "Honey Badger Don't Care," Randall did, and sent a cease and desist letter to Glaister, Zalusky, and Lees. Glaister hopes that an amicable a settlement can be reached. But Honey Badger Sauce raises an interesting legal question: Does Randall have any real claim on this product? National Geographic created the video. His narration certainly made it popular, and the sauce plays off his irreverent sense of humor, but he didn't invent the honey badger, develop the recipe, or promote it. If he deserves a cut, shouldn't National Geographic get a taste as well?

Product licensing is a $187 billion business and as younger generations spend less time watching TV — the usual source of licensable IP — web — and app-based creations will become increasingly popular springboards for products. Just look at this year's ROFLCon, which hosted talks on meme ownership, a decidedly un-ROFL-ey topic.

Beyond the precedent-setting legal matters, the trio also had to overcome more pedestrian concerns like making sure the bottle looked like a fearsome honey badger, not a cuddly honey bear. Luckily, Glaister has a masters degree in industrial design and experience designing kitchen projects that came in handy when working with the mold maker to ensure critical details, like the badger's teeth, made it into production.

None of it matters, though, unless the sauce is tasty. Lees is a keen barbecue chef who could cook up a mean batch of sauce for a cookout, but 10,000 bottles' worth? That meant finding a commercial kitchen, a process Glastier says is "surprisingly straightforward," if a bit slow. The trio provided their recipe and the chef they selected replicated it with production-grade ingredients.

"We went through eight iterations," Glastier says. "The first was terrible, the second was terrible, the third was reasonable, and by the last one it was perfect…. We ate the entire bottle in the car park of the kitchen."

Fans of the honey badger know that it just takes what it wants, but if you want to try the sauce, it's currently raising funds on Kickstarter.

Bibliografia Adicional

COTTER, Thomas F. Memes and Copyright. Tulane Law Review, Vol. 80, 2005. Disponível em:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=826465

LEMOS, Ronaldo ; Branco, S.. COPYLEFT, SOFTWARE LIVRE E CREATIVE COMMONS: A Nova Feição dos Direitos Autorais e as Obras Colaborativas. Revista de Direito Administrativo, v. 243, p. 180-210, 2006

SCHWABACH, Aaron. Reclaiming Copyright From the Outside In: What the Downfall Hitler Meme Means for Transformative Works, Fair Use, and Parody. Buffalo Intellectual Property Law Journal, 2012. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2040538

CAPÍTULO 6 — DEMOCRACIA ONLINE E DESENHO INSTITUCIONAL

CENTRALIZED AND DECENTRALIZED GATEKEEPING ONLINE: POLITICAL DISCOURSE AND MOBILIZATION ON DAILY KOS

Aaron Shaw

ABSTRACT

This paper presents a mixed methods study of gatekeeping in a large online community: the U.S. political blog "Daily Kos." Using qualitative evidence as well as statistical analy — sis of a large sample of comment threads on the site from 2008, I argue that gatekeeping on Daily Kos takes centralized and decentralized forms, and that both modes depend critically on relational boundary work among members of the community. Centralized gatekeeping proceeds through actions by elite and high status members of the site community. Decen — tralized gatekeeping, by contrast, consists of more numerous and small scale interactions between community members. Both forms of gatekeeping serve to enhance the ability of high-status members of the community to control access to privileges and agenda-setting responsibilities on the site. These findings imply that the egalitarian and democratic ethos of "open" online collectives exists in tension with a variety of mechanisms through which participation and status inequalities emerge among participants.

Keywords: Politics, Internet, Media, Gatekeeping, Inequality, Organizations, Social Movements

INTRODUCTION

Online modes of political participation have spurred overlapping debates about the Internet's po — tential to transform political engagement and the public sphere. Some observers herald the de — mocratizing potential and egalitarian character of large-scale online communities and collaborative 1 platforms, such as political blogs or social network sites (SNS). Others have questioned the idea that networked communication over the Internet has altered or overcome underlying social inequal — 2 ities that ultimately determine who gets to participate in the public and political sphere. In these debates, the institutional and organizational dynamics internal to online communities engaged in political action have not received sustained analytical attention. The extensive body of existing research on democratic engagement, media, and the public sphere has demonstrated that such orga — nizational and institutional dynamics play a central role in determining both the success or failure 3 of movements as well as the socio-political implications of particular forms of social organization.

In this paper, I conduct a mixed-methods analysis of the micro-dynamics of interaction within a large-scale political community online. Specifically, I focus on the practices of gatekeeping in 4 the U.S. political blog, Daily Kos. Arguably the largest and most prominent participatory political blog in the U.S., Daily Kos embodies several core aspects of the practices online engagement and 5 participation occurring in the blogosphere. The massive scale of participation on Daily Kos creates a set of coordination and information filtering problems which the site, as a networked organization, "solves" through a distributed system of content moderation and filtering. In contrast with earlier modes of media production and with more hierarchical, exclusive forms of blogging, this system does not rely exclusively on the actions of individual elites in key choke-points of bureaucratic authority to perform centralized gatekeeping roles. Rather, Daily Kos also relies on the collective wisdom of its community of participants to filter the content contributed by their peers.

The key organizational dynamic in such a system of distributed filtering and moderation emerges as a pattern of decentralized gatekeeping, whereby practices of boundary work and social closure take on a more collective, distributed aspect than in previous forms of media production and political organization. In contrast with "traditional," centralized gatekeeping, which proceeds through actions by elite members of a collective or organization, decentralized gatekeeping, con — sists of more diffuse, small scale interactions between community members. Once aggregated, these small scale interactions enhance the ability of high-status members of the community to con — trol access to privileges and agenda-setting responsibilities on the site. In this way, decentralized gatekeeping practices contribute to the emergence and reproduction of status inequalities within Daily Kos that reinforce the site's mechanisms of information filtering and mobilization. Not only content, but also people become the objects of gatekeeping practices on the site.

Gatekeeping on Daily Kos has both centralized and decentralized elements, and in both cases, site participants tend to negotiate status and influence on a relational, discursive basis, rather than on the basis of bureaurcratic hierarchy or formal organizational structure alone. Such patterns of organizational behavior matter for two reasons. First, the surge in online modes of political engage — ment and tools suggests that Daily Kos and other online-centered movements represent new "lab — oratories of democracy" in the Tocquevillian sense. As an increasing number of social movement organizations, political parties, and private firms adopt online tools for collaboration and collec — tive action, the organizational and behavioral dynamics of online collectives become more relevant for the study and practice of public engagement. If the adoption of these tools bring with them novel organizational governance practices or disciplinary mechanisms, these phenomena portend

a broader transformation of the organizational basis of democratic politics. They can also shed light on other, offline environments — such as political parties or social movement organization meetings — in which relational, discursive mechanisms play a role in determining hierarchies of status and influence as a collective seeks to mobilize consensus around a common objective.

The second reason why online gatekeeping matters concerns the character of the sort of partisan movement organization — engaged in media production, mobilization and information dissemination — that Daily Kos exemplifies. The the flow of attention, influence, and status in these new media organizations will shape democratic politics and the networked public sphere in comparison with the mass mediated public sphere. As the blogosphere has grown and become a stable part of the political ecosystem in the U.S. over the past five years, the processes by which ideas and individuals achieve visibility within blogs and related online movements remain opaque. This study sheds light on gatekeeping processes within one of the largest, most dynamic political blogs with the objective of contributing to a wider debate about the politics of news and information production in the contemporary era.

POLITICAL BLOGS AS POLITICAL ORGANIZATIONS

The U.S. political blogosphere emerged during the 2004 presidential campaign. Since that time, the landscape of political blogs has undergone several dramatic shifts as well as a series of some — what more subtle evolutionary changes. The most significant, ongoing transformation has been the formalization and professionalization of the most prominent individuals and organizations in — volved in political blogging. As part of this process, the political blogosphere has become integrated into the organizational networks of the press, the political parties, and the diffuse collection of non — profits, consulting firms, and political action committees that make up the wider sphere of American 6 politics. As an organizational field, the blogosphere has stabilized to a large degree; however, im — portant differences characterize elite blogs on the left and right, corresponding to distinct models of democratic political organization and discursive production in the public sphere.

The first political blogs were highly amateur affairs, and usually consisted of the writings of a well-informed, outspoken political outsider with passionate views. Some blogs, especially MyDD and Daily Kos on the left, made an effort to incorporate multiple contributors and voices into the 7 conversation, but these were the exception rather than the rule. This began to change around the time of the 2004 presidential campaign as the blogosphere emerged as a viable medium of 8 opinion-generation, news diffusion, muckraking, and mobilization. On the left, bloggers played a crucial role driving the Howard Dean campaign in the Democratic primaries and upen-

ding South 9 Carolina Senator Trent Lott in response to a racist remark at a fundraiser. On the right, bloggers helped reveal that CBS News and Dan Rather had used fraudulent documents about George W. Bush's record in the Texas Air National Guard, resulting in a subsequent investigation and hastening 10 Rather's retirement In each of these cases, "A-list" bloggers proved themselves at least equal to journalists in more traditional formats and organizations. In general, they benefited from the speed of publication and transparency norms that characterized the blogosphere from its earliest days. Without the burdens of hierarchical organizations or editorial oversight, the bloggers framed issues and pursued stories in a provocative way that many print, radio, and television journalists were simply unprepared or unwilling to do. As a result they accrued credibility as well as the attention of the public, the media, and political elites.

During these early years, political bloggers were routinely derided as pajama-clad voices from 11 the political wilderness. However, the early elite bloggers resembled their peers in the media and 12 political institutions in terms of educational credentials, class, race and gender. Furthermore, in the years between 2004 and 2008, numerous "first wave" political bloggers received book deals or were hired as columnists by national publications looking to build online traffic and advertising 13 revenue. As time went on, more A-list bloggers could be found on Sunday morning political talk shows or authoring op-eds in major news outlets. As the bloggers professionalized, substantive differences between them and news producers in partisan broadcast print or television media became less salient.

Blogging organizations also became more formal during this time. Most of the early blogs utilized off-the-shelf blogging software and were authored by individuals. For example, of the fourteen unique sites counted as top blogs in 2004 by Drezner and Farrell, only four were either (part of) an incorporated organization or had a formal hierarchy. Of those same fourteen blogs and bloggers, all of them are now either independent entities with formalized corporate status or part of incorporated organizations. This pattern holds across a larger sample of top blogs as well. Data collected by Shaw and Benkler in Summer, 2008 show that at that time, 93 out of 155 (60%) of top political blogs were either (part of) an incorporated entity or involved a formal organizational 14 hierarchy.

Bloggers and blog communities have also integrated themselves into the broader field of es — tablished political organizations, networks and actors. While this process has followed an uneven pace, a number of bloggers on the left and right have become prominent figures within a mobi — lizations and campaigns, signaling their growing role as power brokers and agenda setters. On the right, bloggers at first largely integrated into existing organizations or movements by working with major partisan media outlets (e.g. the

National Review and Fox News), or by forming new media 15 strategy and campaign consultancies. As a result, the right political blogosphere cannot claim leadership of a clearly defined grassroots movement or constituency, but it remains an active force in shaping the voice and agenda of conservative politics. In contrast, the left blogosphere elites have more aggressively sought to transform the landscape of political mobilization through the creation of new organizations and constituencies under the banner of a "netroots" movement. These efforts have proceeded by means of conferences, fundraising campaigns, and new advocacy organizations 16 agitating for change within the Democratic Party.

The processes of professionalization, formalization, and political integration occuring in the blogosphere between 2004-2008 have not followed an even trajectory across all blogs, but have nevertheless resulted in an overall stabilization and institutionalization of the field. Many of the elite blogs established consistent styles and regular communities of reader-participants despite the ebb and flow of attention that follows the electoral calendar. This pattern of stabilization has also manifested in the distribution of attention across the blogosphere as a whole. Using secondary data gathered by Karpf, a comparison of the mean monthly rank of top 50 left and right blogs along sev — eral metrics of authority and attention from June, 2009 through January, 2011, shows the distribution 17 of ranks across left and right blogs to be stable, despite some within group turnover. Correlations between blog rankings for all sites on all measures in the first and last months of Karpf's data col — 18 lection are likewise positive and significant. Both of these results imply that the ecosystem of blogs, while still new and innovative relative to the wider field of political organizations, may not be as volatile as casual observers would believe.

Nonetheless, important differences have emerged between the left and right of the blogosphere. Most significantly, cross-ideological variation in the adoption of participatory blogging platforms 19 has resulted in "two blogospheres" characterized by distinct democratic affordances. Similarly, as implied above, the elite bloggers on the two major sides of the political spectrum have taken divergent approaches when it comes to integrating their discursive production into a broader project of mobilization and movement building. The significance of these cross-ideological differences hinges on whether they facilitate distinct pathways of influence and engagement, as well as the extent to which they do or do not become institutionalized over time.

DYNAMICS OF CONTROL IN OPEN (ONLINE) COLLECTIVES

Many of those who claim that networked movements hold the potential to democratize political dis — course and participation ground their arguments on the view that online collectives do not simply reproduce existing, offline inequalities, but rather enable new publics to coalesce and mobilize

in a 20 more egalitarian fashion than was historically feasible. Counterarguments have underscored the 21 persistence of socioeconomic and other socio-structural inequalities as predictors of participation. Some have also leveled criticism at the design of technical systems that algorithmically reproduce 22 preexisting inequalities of attention and prestige. The question of what sorts of mechanisms of influence and control prevail within online collectives remains unresolved in these debates. The fact that online tools might make enhanced collaboration and participation possible does not determine the outcome. Likewise, even if the mechanisms driving selection into participatory, collaborative online movements tend to reproduce offline inequalities of access or attention, that does not fore — close the possibility that those online movements could still embrace a more open and democratic character than their predecessors. Answering these concerns more precisely requires closer investi — gation of the internal dynamics of control within online collectives.

In organizational terms, Daily Kos and participatory online collectives have a great deal in com — mon with other networked and "open" community organizations, such as those that produce Free 23 and Open Source Software, Wikipedia, or peer-to-peer file sharing groups. However, existing explanations of how these communities work tend to draw primarily on institutional, behavioral, and transaction cost economics as well as social psychological theories of motivation. Specifically, Benkler, Lerner and Tirole, and Weber have all argued that distinct features of digitally-networked information production enable large-scale, "non-market" systems to overcome the obstacles to col — 24 lective action, public goods creation, and sharing identified by classical economic theory. These claims originated as rejoinders to longstanding debates on "the tragedy of the commons" and col — 25 lective action failures in the context of public goods creation. As such, their authors view the fundamental puzzle of commons-based production online as a two-fold question: Why do individu — als make contributions to online collective goods in the absence of financial incentives and how do large numbers of individuals coordinate and sustain their contributions in the absence of either for — mal organizational structures or markets? Their answers to these questions then tend to emphasize relatively static sets of norms, incentives, and motivational profiles. As a result, they overlook the importance of both the structural dynamics within online communities as well as the interactions between community members. Such accounts cannot explain the emergence, transformation, and reproduction of hierarchy or community institutions.

Dynamics of social reproduction, governance, and institutionalization within online collectives all entail a complex set of relational processes emerging through the interactions of community members, who actively manage

organizational boundaries. For example, the work of O'Mahony and Ferraro shows that, over time, the growth of the Debian Linux community has led the commu — nity members to negotiate and implement a steadily more and more complex boundary-management 26 process, leading to increasingly formalized and hierarchical governance structures. Somewhat paradoxically, these formal and exclusionary structures are combined with direct democratic insti — tutions which work to preserve the project's formal openness. The preservation of certain kinds of direct democracy thus appears to support the cultivation of formal organizational structure. The pattern adheres loosely to Michels' "Iron Law of Oligarchy" and reproduces a similar sort of emergent hierarchy to that identified in Freeman's critique of the tyrannical "structurelessness" of the 1970s 27 U.S. Feminist movement.

Such questions of organizational governance and democracy reconnect this line of research with analyses of online social movement organizations and democratic political mobilization. Several previous studies have argued that the emergence of networked, politically-engaged collectives col — laborating over the Internet have transformed the structure and dynamics of the public and political 28 spheres. However, among the body of research analyzing online political movements more specif — ically, only Karpf offers a typology of networked political organizations or a theoretical framework for thinking about the evolution of such communities in relation to existing political movement 29 organizations. For Karpf, political organizations with strong online organizing components hold much in common with their pre-Internet counterparts. The lower communication costs enabled by networked communication have facilitated less hierarchical internal structures, leading to a generational shift as new advocacy organizations on the U.S. left have embraced these possibilities.

Nevertheless, the literature on movement organizations' use of networked technologies and strategies also has a blindspot when it comes to providing more general accounts of how these supposedly "new" practices of less hierarchical mobilization proceed. Keeping with the previous example, Karpf theorizes about the "phases" of growth that the new generation of Internet-savvy organizations pass through, but he does not analyze this process in much depth, nor does he explain the relationship of the organizations' internal dynamics to their apparent "product" in many cases: a complex social system that generates and disseminates a vast amount of political information.

In this regard, research into the micro-social dynamics of these sorts of networked communities provides further insights into the organizational and political dimensions of increasingly popular practices of online collective action and distributed information processing. Online collectives en — gaged in political mobilization constitute novel sorts of institutions, movement organizations, and 30 fields of power with characteristics that resemble their

purely "offline" predecessors. Inquiry into the mechanisms of agenda setting and influence within online collectives can therefore inform a broader analysis of the changing nature of contemporary modes of collective action and politi — cal mobilization. Gatekeeping represents one particularly salient mechanism that has not received adequate attention in the context of online collectives engaged in (political) discursive production.

GATEKEEPING AND BOUNDARY WORK IN THE NETWORKED PUBLIC SPHERE

Along with Google and sites that sort and filter information by means of algorithms, Daily Kos embodies a key aspect of the broader shift towards distributed, social information processing online. This shit, in addition to altering the terrain of social movements and political mobilziation, has also 31 transformed the structure and dynamics of the public sphere. In a context where attention becomes a scarce resource subject to intense competitive pressures, social mechanisms of agenda setting and influence have acquired enhanced importance. Explaining how social processes such as gatekeeping may or may not undergo transformations in online movements and news organizations can clarify what the rise of networked communication means in relation to the organizational and informational dynamics that characterized the mass-mediated public sphere.

Early studies of gatekeeping focused on individuals who held extraordinary control over flows 32 of goods, ideas and attention within families, groups, or society as a whole. Over time, gate — keeping research focused on the role of elites within newspapers, television and other information — producing professions. Practices of gatekeeping by editorial staff inside news--making organiza — tions have historically drawn special attention as the quintessential examples of how institutional, 33 cultural, and organizational dynamics influence what in fact becomes "news" in the first place.

More recent gatekeeping research has likewise focused on journalism and media production, but has shifted to consider the role of institutions, processes, and the structural dimensions of social 34 relations in driving the movement of information and access to resources. A few studies have 35 specifically examined gatekeeping in the context of online collectives and communities. In ad — dition, several studies have explored analogous processes to traditional gatekeeping that likewise structure the dissemination of information in networked environments. Boczkowski's ethnography of networked newsrooms in Argentina illustrates how the adoption of online publication, content aggregators, and the intensified competition for reader attention in a flooded information market — place have transformed the physical and organizational practice of newspaper production, resulting 36 in less diverse content. Hindman's analysis of "Googlearchy" argues that the combined effects of power laws of attention online together with many Inter-

net users' increasing reliance on algo — rithmic information filtering is likely to produce an extremely small elite capable of dominating the 37 networked information ecosystem. In contrast, Benkler and collaborators have argued that the presence of such power laws do not eliminate the possibility that the Internet could be used to de — mocratize political communication, but they also note that the actually existing conditions of online 38 discursive production remain to be studied in great depth.

From a theoretical perspective, these studies have not explained the ways in which gatekeeping or related processes form part of the diffuse dynamics of contention and negotiation that go into managing open online collectives. In these environments, the struggle for attention and influence among the numerous participants means that gatekeeping is as much about inequalities in the at — tention and influence that accrue to particular people as well as to particular types of content. In other words, gatekeeping in open collectives becomes a means of constructing normative boundaries around legitimate discourse and action, and restricting the voice of those who do not adhere to the norms. In this aspect, gatekeeping constitutes a specific form of relational boundary work 39 in the service of elite "status closure". Such relational work encompasses the diverse repertoire of practices through which individuals and groups define, imitate, contest, and reconstruct social categories. These practices also serve as the everyday mechanisms through which categorical in — 40 equalities, social movements, and economic exchanges cohere into larger structures. As part of a broader repertorie of organizational governance practices, relational boundary work among the participants in online collectives simultaneously drives the emergence of formal hierarchy at the same time that it enables the preservation of open, democratic institutions.

The dynamics of coordination and organization in large-scale online communities that generate, filter, and disseminate information on a massive scale offer a compelling arena for further studies of networked gatekeeping. Despite the growing number of sites on the Internet that fit this descrip — tion — prominent examples include Daily Kos, Reddit, Digg, and Slashdot — only a few studies have attempted to characterize the social dynamics of information filtering within these sorts of 41 networked communities. My study of Daily Kos contributes to this body of research by extending the analysis of gatekeeping to incorporate an analysis of centralized, elite-level gatekeeping as well as the decentralized, relational practices of social information filtering and production pursued in large networked communities. A relational perspective focused on diffuse micro-level interactions expands existing theories of gatekeeping beyond the traditional focus on central choke points of 42 control. The central points within organizational hierarchies or networks traditionally identified as the locus of gatekeeping activities remain significant, but (in the context of open or network organizations) gatekeeping practices

occur throughout a collective. In this sense, some kinds of gatekeeping may be more decentralized in character and a distributed form of social control rather than a form of top-down coercion.

At its core, decentralized gatekeeping consists of numerous, micro-level interactions between individuals engaged in a particular collective endeavor. Through the aggregation of distributed, relational exchanges, which draw on existing rhetorics, norms and codes of behavior, these individ — uals participate in the stabilization and reproduction of larger scale social dynamics. Over time, this process results in wider patterns of path dependency and creates institutionalized impediments to sudden shifts in the social order. Thus, with or without the central points of control through which traditional practices of gatekeeping proceed, organizations or communities constituted through dis — tributed social interaction have a tendency to generate the sorts of deeply entrenched hierarchies 43 and structures identified in earlier work on democratic, open or "structureless" organizations.

(…)

CONCLUSIONS

The results presented here suggest the presence of multiple kinds of gatekeeping on Daily Kos, both of which may have contradictory effects on the site. Collective action in a large and "open" online community entails more than the boundary work traditionally conceived as centralized gatekeeping by site elites and administrators: it also relies on participants' decentralized interactions, which give rise to gatekeeping effects and status inequalities. These effects and inequalities, in turn, feed back into the complex of norms, practices, and standards that prevail among site users, contributing to the community's overall political activities as well as the continuity of its social dynamics.

Gatekeeping practices by participants on Daily Kos thereby contributes to the emergence and reproduction of inequalities on the site. My examples illustrate how high-status contributors to Cheers & Jeers performed boundary work in moderating the comment threads. Sometimes — as with 2NurseLady — they did so in conversation with site elites like Bill in Portland Maine; however, the aggregated evidence taken from the entire archive of 2008 C & J comment threads suggests that the effects also diffuse and decentralized across the user population as a whole. On the basis of this suggestive qualitative and quantitative evidence, future research should pursue more precise identi — fication strategies through which to test for the presence or effects of decentralized gatekeeping.

In the incidents involving joan reports and 2NurseLady, the ability of the community members to moderate successfully depended in part on their ability to draw on and deploy appropriate codes of behavior established on the site. In deploying these codes, they enacted informal community norms whi-

ch validated contributions consistent with the overarching goals articulated by Moulitsas, Harnsberger and other site elites elsewhere. When necessary, they also adapted existing standards to suit the needs of particular situations.

Across these examples, the distinction between centralized and decentralized gatekeeping is porous, and there are many ways in which Moulitsas' and other site elites' actions influence the patterns of gatekeeping that prevail across the rest of the community. The effects of decentralized gatekeeping are, in some sense, the cumulative result of many small-scale examples of relational boundary work, each instance of which involves much smaller numbers of people in specific interactions. Among the site elites and leaders, the tendency towards social closure and exclusion must continually be balanced against the ideological and organizational exigencies to egalitarian and democratic ideals. As 2Nurselady demonstrated, appeals to such ideals — even when made by someone who does not appear to have a long-term commitment to the site — are taken seriously.

The mechanisms of gatekeeping described here only reflect a snapshot of a single dimension of participation (commenting) on the Daily Kos site during a specific period of time. Patterns of decentralized gatekeeping and path dependency reinforced through comment recommendation are therefore not deterministic of the social structure among the site's community as a whole. Making comments and receiving recommendations is far from the only means by which members of the site might participate and acquire status in the eyes of their peers. There are also user-blogs (di — aries); participation in offline and advocacy events (such as the annual Netroots Nation Conference or unaffiliated social events); as well as work within the formal Daily Kos organization or other organizations that make up the netroots political movement.

In other words, the practices and norms of comment recommendation and the corresponding patterns of path dependency that appear to go along with comment recommendation constitute a single dimension of the multiplex social processes through which status hierarchies may emerge, rise and fall within Daily Kos as a whole. Reputational gains through commenting thus do not guar — antee that a given user of the site will become well--known or achieve broader influence, although they are an index of a certain kind of reputational standing. In this way, status achieved or measured through comments is not determinative of other sorts of status within the community. However, comment recommendations do provide a visible and objective indicator of one dimension of the community's status relations. More fine-grained longitudinal analyses of the patterns of comment posting and recommendation in relation to other modes of status acquisition would be necessary to establish the precise mechanisms by which Daily Kos participants become more or less influential members of the community. Also, fur-

ther analysis will be necessary to establish whether or not the oligarchic tendencies revealed by this analysis persist across these other forms of behavior.

To the extent that the patterns of decentralized gatekeeping through comment recommendation analyzed here constitute a path dependent system of status relations, they imply several conclusions relevant to theories of gatekeeping, democratic organizations, and the networked public sphere. First of all, the presence of decentralized gatekeeping complicates the "myth of digital democracy" perspective elaborated by Hindman and others that views the online public sphere as nothing more 75 than a new setting in which old elites can exert their influence. Just as traditional social movement organizations cannot be defined in reference to the identities of their leaders alone, it does not make sense to characterize Daily Kos as an extension of the personality traits of Markos Moulitsas. In moments of conflict, Moulitsas may draw on his monopolistic control over the site infrastructure as a rhetorical justification for the legitimacy of his perspectives, but both he and the other site elites ultimately rely on the persuasiveness of their rhetoric and their ability to build discursive consensus. In this sense, the processes and practices of gatekeeping reinforce the democratic basis of the site — only the best contributions receive broad support — at the same time as it serves the interests of those who already possess status and influence within the community.

Indirectly, decentralized gatekeeping dynamics reinforce Hindman's view that hierarchies, sta — tus and social reproduction may emerge through the network dynamics of communication and participation in the open and non-bureaucratic organizations of the blogosphere. In this sense, even though Daily Kos may be unique in terms of its scale and recognition in the political blogo — sphere, the site may exemplify patterns of attention, influence, and participation found within open source software development communities, Wikipedia, networked social movement organizations, and other sorts of open collective action projects. If decentralized gatekeeping prevails across these other kinds of environments, those who would equate openness with egalitarian outcomes must reconsider their position. Decentralized gatekeeping may represent yet another pathway towards inequality production within the larger sphere of democratic and online participation even at the same time as it introduces a means for a new elite to achieve prominence within particular sites or 76 movement organizations.

This analysis of gatekeeping in Daily Kos also reveals some of the variations that characterize gatekeeping in networked environments in contrast with their offline counterparts. Previous studies of offline gatekeeping have focused on bureaucratic settings with fairly clear boundaries. These settings have given rise to modes of gatekeeping behavior largely consistent with the organizational affordances and constraints particular to each environment. For example, newspaper editors exercise individual and collective authority

over what sorts of news makes the front page. Likewise, tenured faculty at research universities review grant proposals to determine which projects will receive funding and institutional support. In both cases, incumbents or elites establish and enforce norms that enable them to manage the boundaries of a particular field. In addition, the gatekeeping might proceed at either an dividual or a collective level. A single editor makes choices about articles that go into her particular section and newspaper, and she also attends conferences and social events where industry-wide standards are discussed among her fellow editors.

Gatekeeping mechanisms in online collectives like Daily Kos have similar dimensions to these other, offline settings. Moulitsas, the other site elites, and some of the well-recognized incumbent users may hold the authority to directly shape and enforce the sorts of behavior that are considered legitimate on the site. In particular, Moulitsas' unique role as the site's figurehead as well as his ab — solute authority over the site's infrastructure provide him with broad dictatorial powers, although he 77 seems to avoid using them to their full extent. At the same time, the collective gatekeeping prac — tices also take on a more decentralized character as the practice of deploying categories of behavior and enforcing norms is distributed more widely across the community. While this study has char — acterized these decentralized gatekeeping effects and found quantitative evidence of their presence on an aggregate scale, my findings cannot speak to the effects of decentralized gatekeeping on ei — ther the character of political discourse or political engagement. Other studies have addressed these 78 issues, but more research will be necessary to evaluate whether and how such transformations matter for the future of political engagement, news production, and collective action.

A theoretical and empirical account of decentralized gatekeeping thus represents a useful coun — terpoint to previous work emphasizing the salience of participatory affordances within the net — 79 worked public sphere in general and the political blogosphere in particular. Institutionalized status inequalities inside of open online communities contradict some of the radical egalitarian ideals that make these sites attractive to many people at the same time as they facilitate long-term movement building goals and the continued commitment of community insiders.

The establishment and preservation of an elite minority within open online collectives may serve an analogous purpose to the stabilization of management structure and roles in more traditional organizational forms. Elite community members can provide continuity as well as a baseline of contributions to the site at the same time as they play an agenda-setting role relative to their peers. They can also incorporate less experienced peers into the community through the transmission of 80 norms and training. In the context of political movement building, this kind of leadership can promote

long-term movement survival, the achievement of advocacy goals and other metrics of movement success. In open online collectives, gatekeeping and similar practices may therefore be necessary for the success and survival of the community as it allows for the cultivation of a high signal-to-noise ratio in what would otherwise be a cacaphonous, chaotic environment. According to such a view, the exclusion of certain people and perspectives could serve a productive function inasmuch as it allows for the site to achieve growth and coherence. This would imply a networked corollary to Michel's "Iron Law of Oligarchy." As findings from a single case do not provide an empirical foundation for settling such debates, however, future work should elaborate these claims and test their applicability to a wider range of open online collectives and network organizations.

In terms of the broader field of politics and political organizations in the United States, the patterns of intra-blog stabilization exemplified by Daily Kos coupled with the overall stabilization of the blogosphere discussed earlier suggest that the initial period of disruptive innovation that characterized the political role of the blogosphere between 2004 and 2008 may have already ended. This does not mean that the influence of the political blogosphere and associated movements such as the netroots is waning or diminished, but rather that the place of blogs within the field of U.S. politics and the networked public sphere may no longer be as volatile as it initially seemed. Blogs are now an established piece of the political information and movement ecosystem and it makes intuitive sense that their internal dynamics would likewise assume a relatively stable form. Within the Daily Kos community, the stabilization of a set of norms, hierarchies and elites imply that the community has, in some sense, solved a core problem of movement-building and social reproduction. At the same time, this opens up related questions about the mechanisms of organizational transformation. The dynamics of path dependency discussed here are already playing an important role in shaping the future of the site and its ability to mobilize its membership. It will be important to see whether or not this stabilization extends to the netroots movement and the role of the Internet in political behavior more broadly.

Bibliografia Adicional

DAHLGREN, Peter. The Internet, public spheres, and political communication. Dispersion and deliberation. in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

FARIS, Robert; ETLING, Bruce. Madison and the Smart Mob: The Promise and Limitations of the Internet for Democracy. The Fletcher Forum of World Affairs, 32, 2008.

FISHKIN, James. Possibilidades democráticas virtuais: Perspectivas da democracia via internet. In: EISENBERG, José; CEPIK, Marco. Internet e política: teoria e prática da democracia eletrônica. Belo Horizonte: UFMG, 2002.

FROOMKIN, A. Michael. Habermas@discourse.net: Toward a critical theory of cyberspace. Harvard Law Review, 116, 2003.

HARTMANN, I. A. M.. Ciberdemocracia: A Personalidade Digital e A Motivação para o Engajamento Cívico na Internet. Revista de Direito das Novas Tecnologias, v. 8, p. 67, 2012.

HARTMANN, Ivar A. M. e-codemocracia: A Proteção do Meio Ambiente no Ciberespaço. Porto Alegre: Livraria do Advogado, 2010.

KLEINWÄCHTER, Wolfgang. Internet co-governance. Towards a multilayer multiplayer mechanism of consultation, coordination and cooperation (M3C3). in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

CAPÍTULO 7 — TECNOLOGIA APLICADA AO DIREITO — LAW & BIG DATA, LEGAL ANALYTICS E O CASO DO SUPREMO EM NÚMEROS

ACESSO AO SUPREMO: QUANDO OS RECURSOS SÃO PARTE DO PROBLEMA

Joaquim Falcão
Ivar A. Hartmann

Publicado na Revista Diálogos sobre Justiça, Ministério da Justiça, número 1, ano 1, 2013.

1. Introdução

No início da década de 2000, a carga de trabalho do Supremo Tribunal Federal (STF) alcançou proporções inimagináveis para qualquer corte cujo papel central seja o controle — abstrato ou concreto — de constitucionalidade. A Emenda Constitucional nº 45/2004 foi a resposta, idealizada, discutida e apoiada pelo Legislativo, Executivo e Judiciário para uma série de problemas que assolavam o Judiciário. Um deles atacado pela EC 45 foi justamente a avalanche de recursos que ameaçava paralisar o Supremo. Os mecanismos da súmula vinculante e da repercussão geral foram pensados e depois regulados pelo legislador, passando a valer em 2007.

Assim como as reformas processuais anteriores, o contexto que prevaleceu após a efetiva implementação foi de ausência de estudos que pudessem avaliar estatisticamente o panorama no Supremo após as mudanças.[1] Em 2011, foi lançado no Supremo o I Relatório Supremo em Números — O Múltiplo Supremo.[2] O estudo foi o resultado de uma análise de todos os processos que passaram pelo Tribunal desde 1988 e permitia comparar os três tipos de Supremo que emergiram dos dados: o Constitucional, o Ordinário e o Recursal. Entre as questões enfrentadas pelo I Relatório estava a evolução do Supremo Recursal. Os dados disponíveis até então eram animadores: nos anos finais da década de 2000, o Supremo vivenciou um "tsunami antirrecursal".[3] Já era visível que o Tribunal não estava conseguindo julgar as repercussões gerais que reconhecia, mas a quantidade de novos processos do Supremo Recursal — agravos de instrumento e recursos extraordinários — havia caído significativamente.

Esse era o panorama até 2010, último ano analisado pelo estudo. Mas e depois?

O presente artigo tem por objetivo responder a essa pergunta. Ou seja: qual o perfil do Supremo Recursal a partir de 2011 e até a metade de 2013? Mais especificamente, como evoluiu a quantidade de processos chegando ao Supremo? A quantidade de processos julgados? O assunto desses processos? E o resultado dos julgamentos desses processos?

[1] No que se refere ao Judiciário brasileiro como um todo, a grave falta de tais estudos é similar. Algumas gratas exceções existem, entretanto. É o caso do estudo "Justiça em Números", publicado anualmente pelo Conselho Nacional de Justiça. A pesquisa evidencia o perfil das diferentes esferas e instâncias da Justiça nacional, sob o ponto de vista dos recursos humanos, orçamento, carga de trabalho e informatização do processo, entre outros. Ver CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números*. Brasília, 2011. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/eficiencia-modernizacao-e-transparencia/pj-justica-em-numeros/relatorios>. Acesso em: 29/02/ 2012.

[2] FALCÃO, Joaquim; CERDEIRA, Pablo; ARGUELHES, Diego Werneck. *I Relatório Supremo em Números — O Múltiplo Supremo.* Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2011. Disponível em: <http://supremoemnumeros.fgv.br>.

[3] *I Relatório Supremo em Números*, op. cit., p. 58 e ss.

2. Metodologia

Para responder a essa pergunta, adotamos metodologia de pesquisa empírica, com técnica quantitativa. Os dados foram levantados usando a base de dados do projeto Supremo em Números. Trata-se de projeto de pesquisa do Centro de Justiça e Sociedade (CJUS) da Escola de Direito da Fundação Getúlio Vargas (FGV), no Rio de Janeiro. O projeto realiza macroanálises de todos os processos do Supremo desde 1988. A versão atual da base de dados contém informações sobre 1.488.201 processos autuados, 2.692.587 partes e 14.047.609 registros de andamentos. Os últimos abrangem informações sobre datas e resultados de decisões tomadas durante os processos, entre outras. As informações sobre os processos contêm dados sobre o assunto jurídico atribuído pelo próprio Supremo ao caso.

Pesquisas como esta, envolvendo grandes *data sets*, têm permitido aos juristas analisar de maneira muito mais minuciosa decisões judiciais.[4] Nesse contexto, a disponibilidade de equipamento computacional, software e suporte técnico desempenha um papel-chave na viabilização de estudos empíricos pelos pesquisadores do Direito nos Estados Unidos.[5] A mesma situação prevalece no Brasil, onde faculdades de Direito recém-começam a adaptar-se a essa realidade, tornando o acesso a tal instrumental um elemento ainda mais importante de propostas de pesquisa.[6] Os dados que subsidiam esse artigo, bem como a diversificada produção do projeto *Supremo em Números*,[7] são possíveis somente em razão do uso de ferramental tecnológico potente.

Ademais, a técnica de pesquisa escolhida pretende responder a pergunta delineada acima mediante um olhar do todo — não de decisões isoladas do Supremo. O novo movimento de estudos empíricos[8] no Direito, no qual o presente artigo se insere, sempre se distinguiu do realismo jurídico e da sociologia jurídica em que as pesquisas são preponderantemente quantitativas, e não qualitativas.[9]

3. Resultados

Conforme mostrado no *I Relatório Supremo em Números*, o Supremo Recursal era representado pela carga do Tribunal referente aos Agravos de Instrumento (AIs) e Recursos Extraordinários (REs). A primeira medição feita, portanto, foi para determinar a evolução desse tipo de processo em comparação com os demais. Para isso, produzimos um gráfico (Gráfico 1) com o número de processos autuados por ano de cada tipo processual, desde 2006 (último ano antes da entrada em vigor dos mecanismos da EC 45). Incluímos apenas aqueles tipos processuais que tiveram ao menos 100 processos autuados em 2012.

[4] DIAMOND, Shari Seidman; MUELLER, Pam. Empirical legal scholarship in law reviews. *Annual Review of Law and Social Science*, v. 6, p. 581-599, 2010.

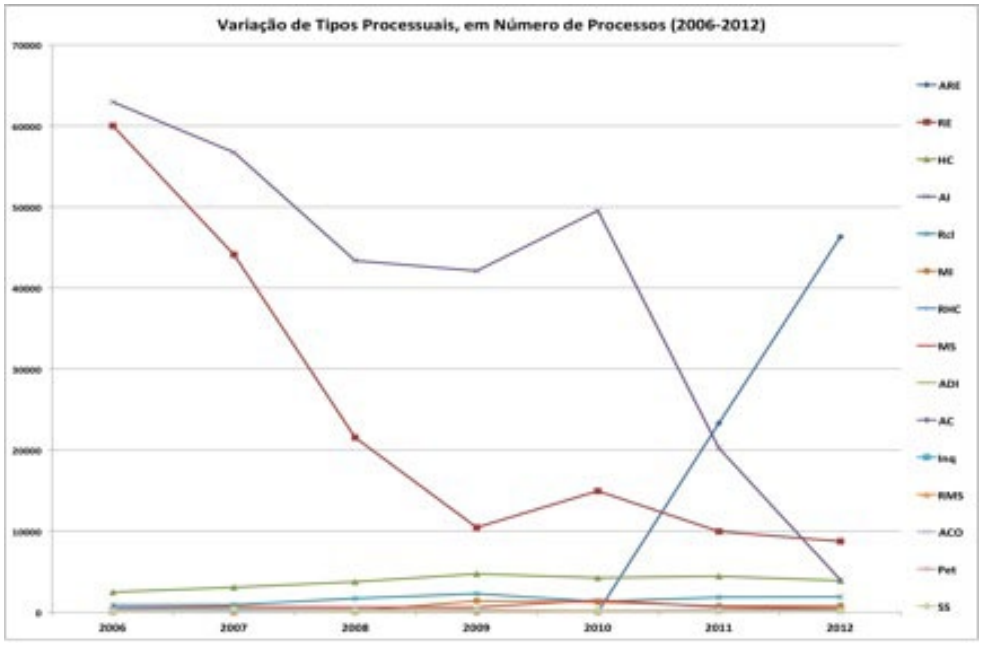
[5] EPSTEIN, Lee; KING, Gary. Building an infrastructure for empirical research in the law. *Journal of Legal Education*, v. 53, n. 3, 2003.

[6] VERONESE, Alexandre. O problema da pesquisa empírica e sua baixa integração na área de Direito: uma perspectiva brasileira da avaliação dos cursos de pós-graduação do Rio De Janeiro. Anais do XVI Congresso Nacional do CONPEDI, Belo Horizonte, 2007. Disponível em: <http:// www.conpedi.org.br/manaus/arquivos/anais/bh/alexandre_veronese2.pdf>. Acesso em: 11/2012.

[7] Ver, por exemplo, FALCÃO, Joaquim; ABRAMOVAY, Pedro; LEAL, Fernando; HARTMANN, Ivar A. *II Relatório Supremo em Números*. O Supremo e a Federação. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2013. Disponível em: <http://supremoemnumeros.fgv.br>. HARTMANN, Ivar A.; AGUIAR, Lucas A. Possibilidade de pedir novo julgamento é controversa. *Folha de S. Paulo.* 16/11/2012. HARTMANN, Ivar A.; AGUIAR, Lucas A. Como o STF deve proceder em caso de empate? *Portal G1*. Disponível em: <http://g1.globo.com/politica/mensalao/traduzindo-julgamento/platb/2012/10/03/como-o-stf-deve-proceder-em-caso-de-empate/>. Acesso em: 22/09/2013.

[8] YANOW, Dvora; SCHWARTZ-SHEA, Peregrine (Ed.). *Interpretation and method: empirical research. Methods and the interpretive turn*. M. E. Sharpe, 2006.

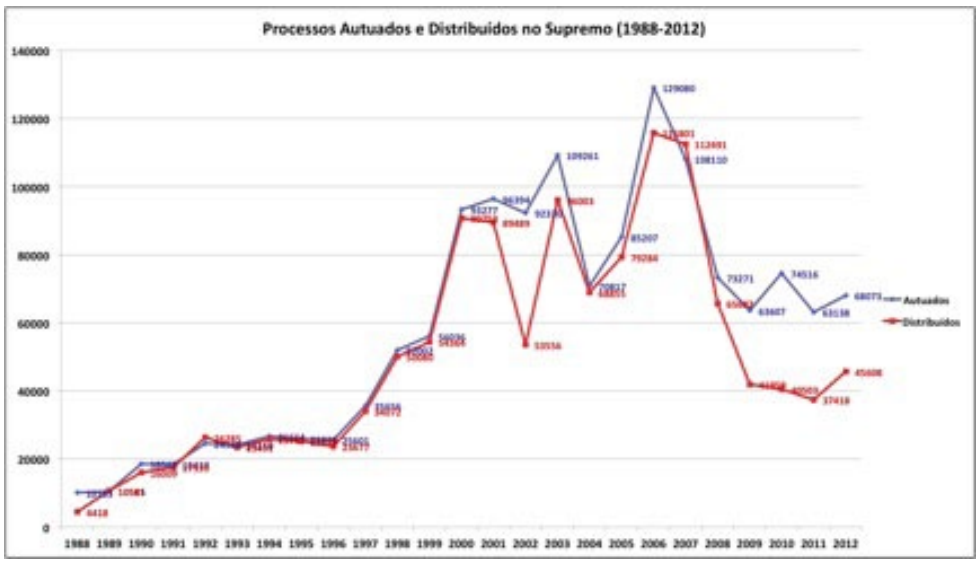
[9] SUCHMAN, Mark C.; MERTZ, Elizabeth. Toward a new legal empiricism: empirical legal studies and new legal realism. *Annual Review of Law and Social Science*, v. 6, p. 555-579, 2010.



É possível notar que, conforme esperado, o número de novos AIs e REs chegando ao Supremo caiu vertiginosamente. No caso dos REs, isso se deu entre 2006 e 2009. Já no caso dos AIs, a queda veio principalmente entre 2010 e 2012. Mas isso não representou uma diminuição no número total de recursos autuados pelo Tribunal. A partir de 2011, um novo tipo surgiu e substituiu principalmente os AIs: o Agravo em Recurso Extraordinário (ARE). O ARE foi implementado a partir de uma reforma ao Código de Processo Civil, em 2010. Ou seja, não se trata de uma categoria processual que sempre existiu, passando a ostentar grandes números somente agora. Ela não existia no Supremo antes de 2011.

Enquanto os AIs e REs representaram 95% de todos os processos que bateram à porta do Supremo em 2006, antes dos mecanismos da reforma do Judiciário entrarem em ação, o ARE alcançou 68% dos processos chegando ao Supremo em 2012. O ARE é o novo Supremo Recursal.

E o que isso fez para a carga total de processos do Supremo? É possível que ela tenha diminuído, mesmo com o surgimento do ARE em grande número. Não parece ser o caso, mas o Gráfico 2 serve como mais um teste para essa hipótese.



Desde 1988, virtualmente todos os processos autuados no Supremo são distribuídos a um ministro relator. O ano de 2002 parece ser uma exceção. Mas a partir de 2008, e principalmente em 2009, passa a existir uma grande diferença entre o número de autuados e distribuídos. A negativa da Presidência do Supremo em distribuir boa parte dos processos que chegam à sua porta fez com que o número de processos repassados aos ministros tenha caído anualmente desde 2006. Mesmo em 2010, quando o número de processos autuados aumentou, o número de distribuídos continuou caindo. Mas em 2012, pela primeira vez em sei6 anos, o número de processos distribuídos aumentou em relação ao ano anterior. E por uma margem significativa: 22%.

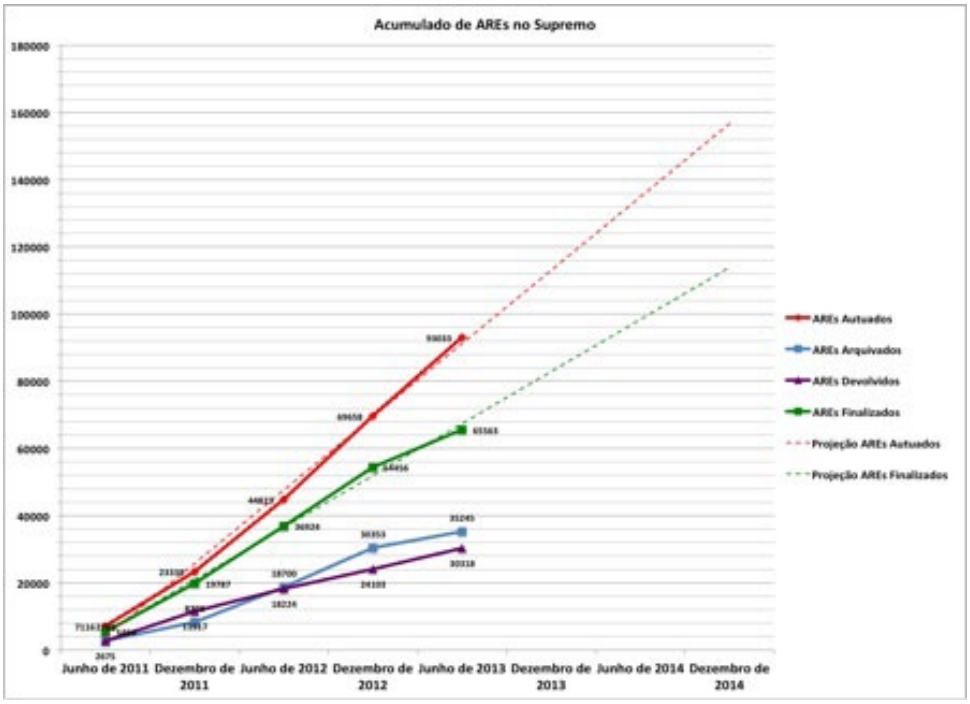
A despeito dessa grande virada, tudo indica que os mecanismos da EC 45 passaram a ser usados pela Presidência do Tribunal ao menos a partir de 2008. Mas como isso se deu no caso dos AREs?

Em 1º de fevereiro de 2011, o Recurso Extraordinário com Agravo (ARE) nº 634.868 foi o primeiro de seu tipo a ser distribuído para julgamento no Supremo Tribunal Federal. Outros quatro AREs foram igualmente distribuídos para julgamento até que, em 14 de fevereiro de 2011, o primeiro foi recusado. Nessa ocasião, o ARE 635.345 foi devolvido ao colegiado recursal dos juizados especiais da Bahia, onde a decisão recorrida havia sido dada. Até aí a proporção foi de cinco AREs aceitos e distribuídos para cada um ARE devolvido.

Qual a proporção quando se olha a totalidade de AREs? Até o final de junho de 2013, foram autuados 93.033 no Supremo. Destes, 45.219 foram distribuídos. Se considerarmos as distribuições por prevenção ou por exclusão de ministros, são 45.951 AREs distribuídos. Trata-se de 49,39% dos AREs autuados.

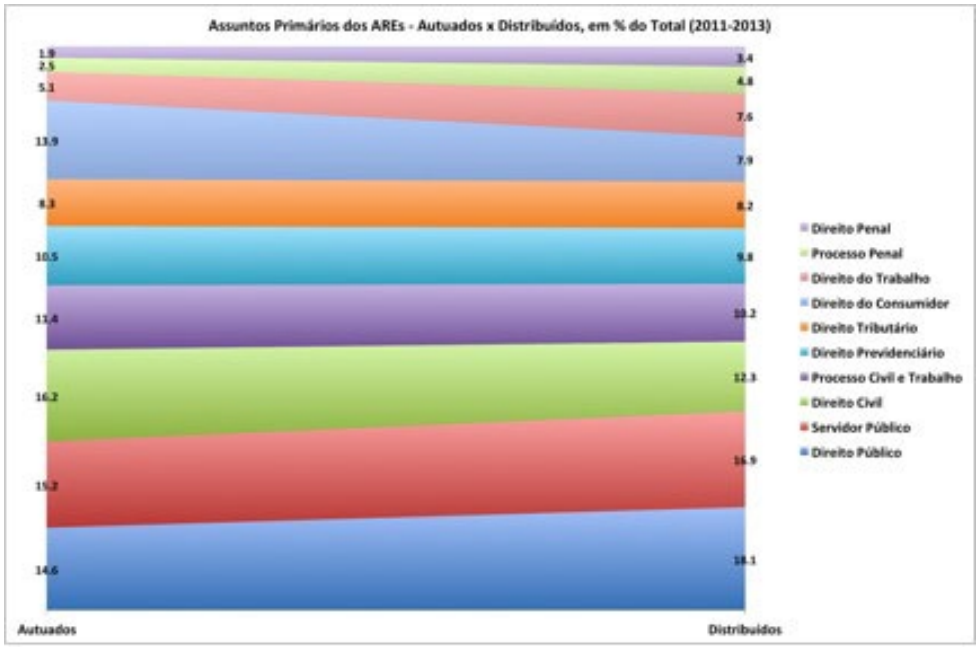
O número total de AREs devolvidos, ou seja, para os quais foi aplicado o art. 543-B do Código de Processo Civil, é de 29.869. Isso equivale a 32,1% de todos os AREs autuados.

O significado disso para a carga de trabalho do Supremo é relevante. É claro que, dos 93.033 AREs autuados até agora, boa parte já foi julgada. Ou sequer foi distribuída, o que significa que não chegará a impactar o trabalho dos ministros. O Gráfico 3 mostra a quantidade *acumulada* dos autuados, devolvidos, arquivados e finalizados (a soma dos devolvidos e arquivados), a cada seis meses, desde o primeiro semestre de existência do ARE. Com a evolução até junho de 2013, são feitas projeções lineares de crescimento desses números acumulados.

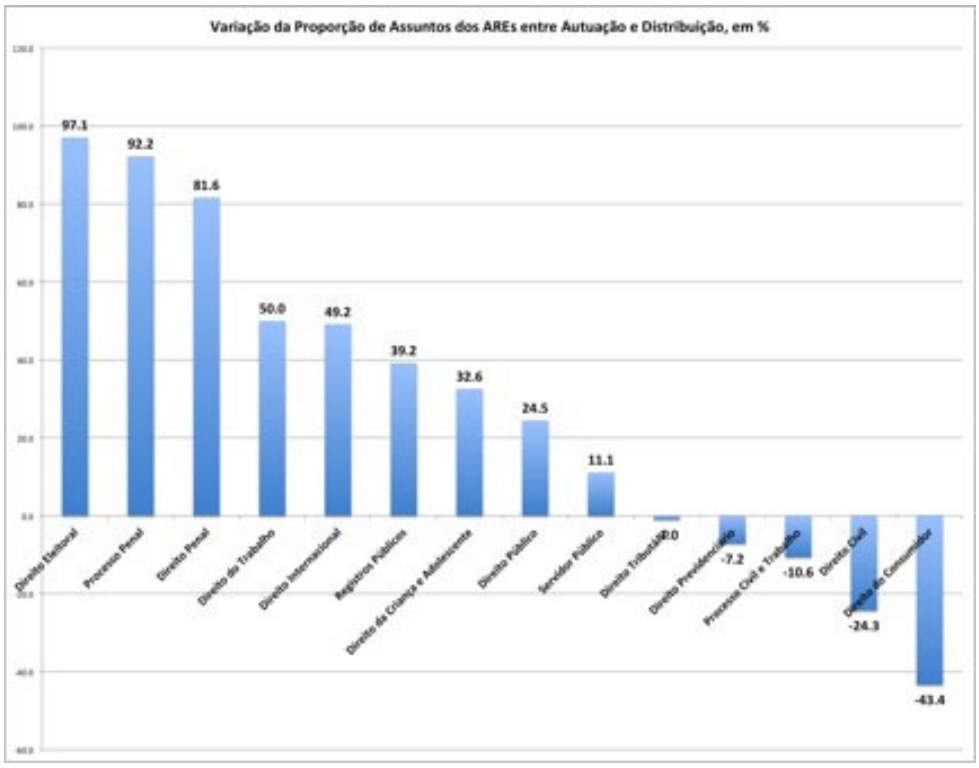


Como se pode perceber, em junho de 2013 o passivo de AREs do Supremo era de 27.470 processos. Seguindo a tendência atual, em dezembro de 2014, esse passivo terá ultrapassado 40 mil processos.

Os três principais assuntos dos AREs são Direito Público, Servidor Público e Direito Civil. Há uma variação entre a composição dos assuntos nos processos autuados e nos processos distribuídos, conforme pode ser notado no Gráfico 4. Este mostra a proporção entre AREs autuados e distribuídos dos assuntos com ao menos 1% do total de AREs distribuídos. Exclui, portanto, assuntos como Direito Internacional ou Registros Públicos.



Essa variação é colocada em evidência no Gráfico 5:



Ou seja, os AREs de Direito Eleitoral ocupam uma fatia 97% maior entre os distribuídos do que entre os autuados. Já os AREs de Direito do Consu-

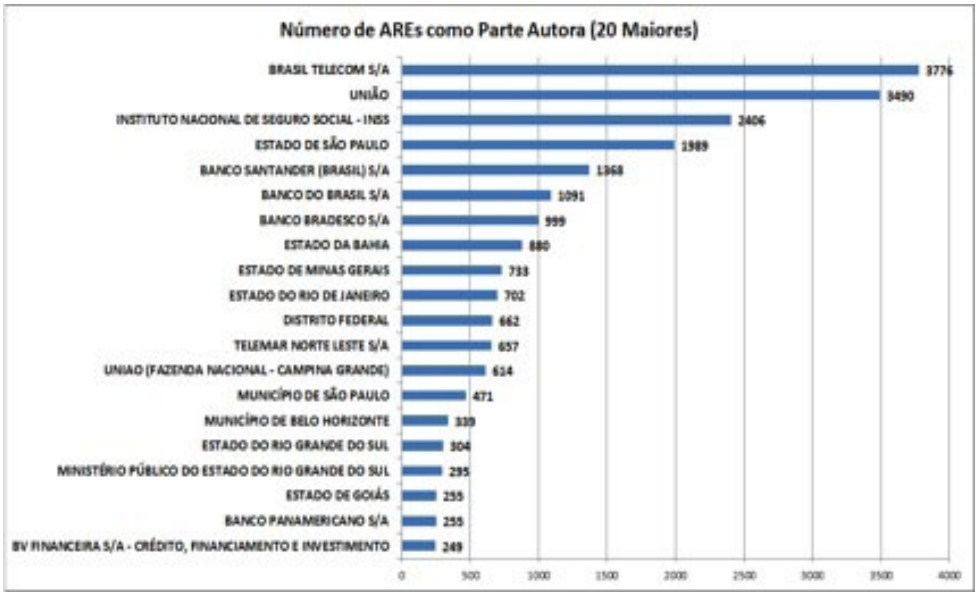
midor ocupam uma fatia 43% menor. Na tabela abaixo, consta o número de AREs de cada assunto.

Assunto	Autuados	Distribuídos
Direito Público	13.302	8.325
Servidor Público	13.924	7.780
Direito Civil	14.833	5.646
Direito da Criança e Adolescente	15	10
Direito do Consumidor	12.681	3.611
Direito do Trabalho	4.638	3.498
Direito Eleitoral	328	325
Direito Internacional	12	9
Direito Penal	1.731	1.581
Direito Previdenciário	9.611	4.487
Processo Civil e Trabalho	10.439	4.691
Processo Penal	2.274	2.198
Direito Tributário	7.568	3.769
Registros Públicos	30	21
Total	**91.386**	**45.951**

O art. 328, parágraf§ único, do Regimento Interno do Supremo determina que ao receber os AREs, se for identificado mais de um recurso "com fundamento em idêntica controvérsia", caberá ao órgão competente junto à Presidência do Supremo selecionar aqueles representativos e devolver os demais.

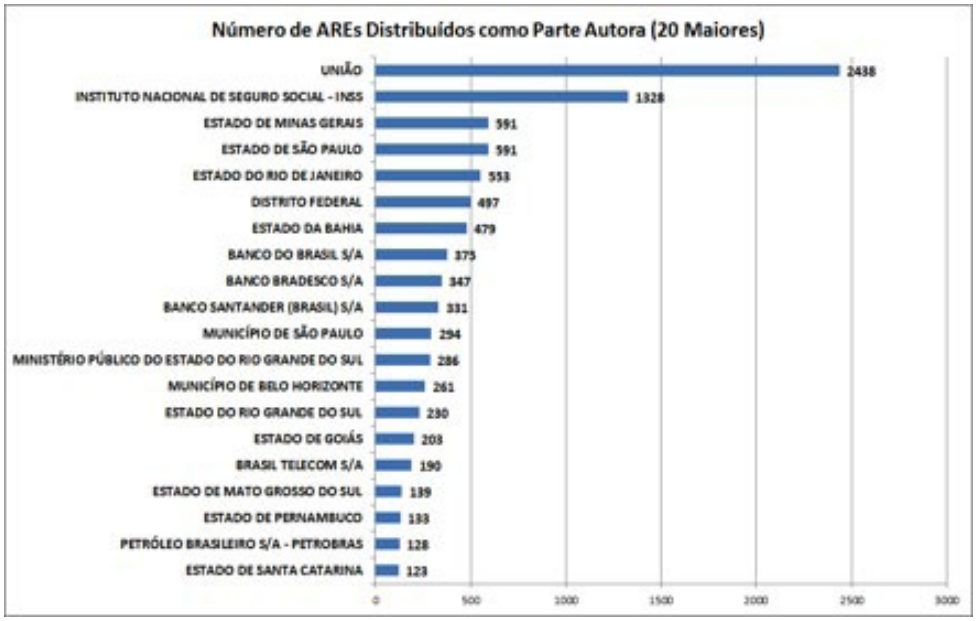
Isso significa que em um período de 30 meses, entre janeiro de 2011 e junho de 2013, o Supremo recebeu nada menos que 8.325 *controvérsias diferentes* de Direito Público. E 7.780 *questões de direito diferentes* sobre Servidor Público.

A identificação das partes autoras desses recursos permite melhor contextualizar os dados sobre o suposto ineditismo dos assuntos submetidos ao Supremo. Contamos a quantidade de AREs em que cada litigante é parte ativa. Ou seja, a que levou o recurso ao Supremo. O gráfico 6 mostra a quantidade de processos autuados dos 20 maiores litigantes.



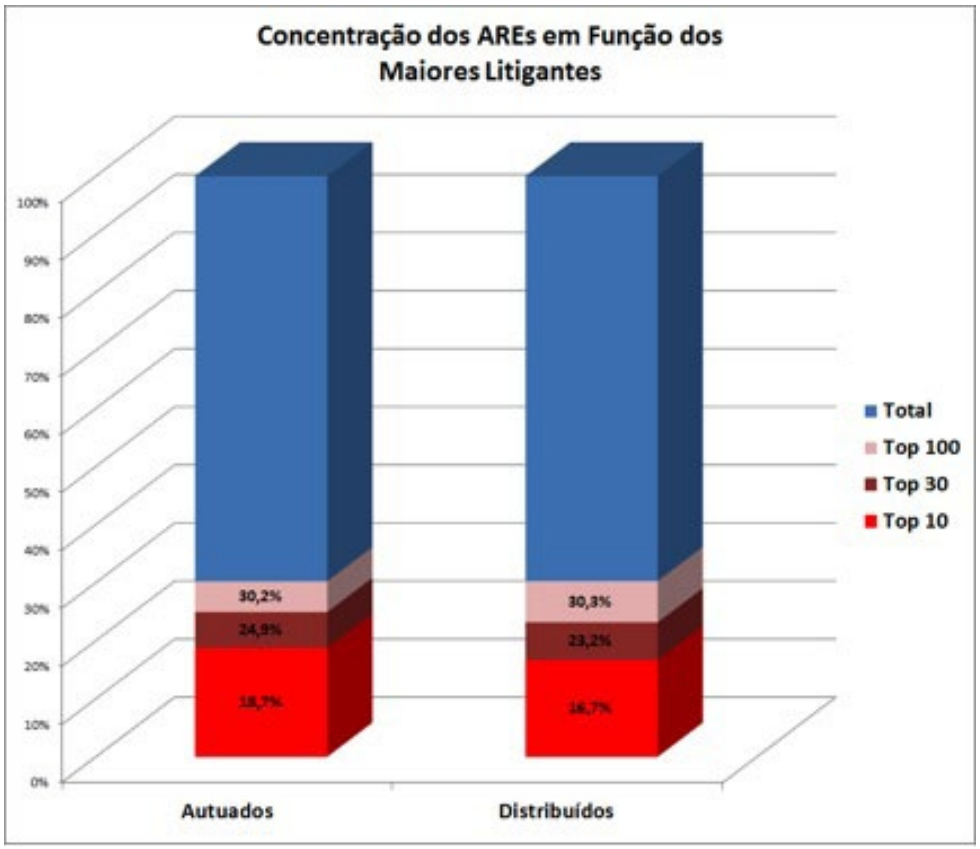
A companhia de telefonia Oi figura em primeiro lugar, como parte recorrente em 3776 AREs autuados no Supremo. A União fica em segundo, com 3490. A concentração dos processos entre os principais litigantes é tal que o Município de Belo Horizonte, 15º colocado, já conta com menos de 10% dos AREs da Oi.

Esses dados, entretanto, mostram apenas quem mais *tenta* ingressar com AREs ao Supremo. Por isso contamos também o número de AREs distribuídos em que cada litigante é parte autora. Os dados encontram-se na figura 7, abaixo.



Em primeiro lugar, com maior número de AREs distribuídos, encontra-se a União — 2438. Já o INSS é parte recorrente em 1328 que foram distribuídos pela Presidência do Supremo. Novamente nota-se grande concentração de processos entre os maiores litigantes. A Oi sai do primeiro lugar e cai para 16º. De modo geral os entes estatais mantêm suas posições, ao passo que as empresas privadas caem.

Verificamos a quantidade de AREs dos maiores 10, 30 e 100 litigantes tanto entre os autuados, quanto entre os distribuídos. A concentração em ambos os universos é mostrada no gráfico 8.

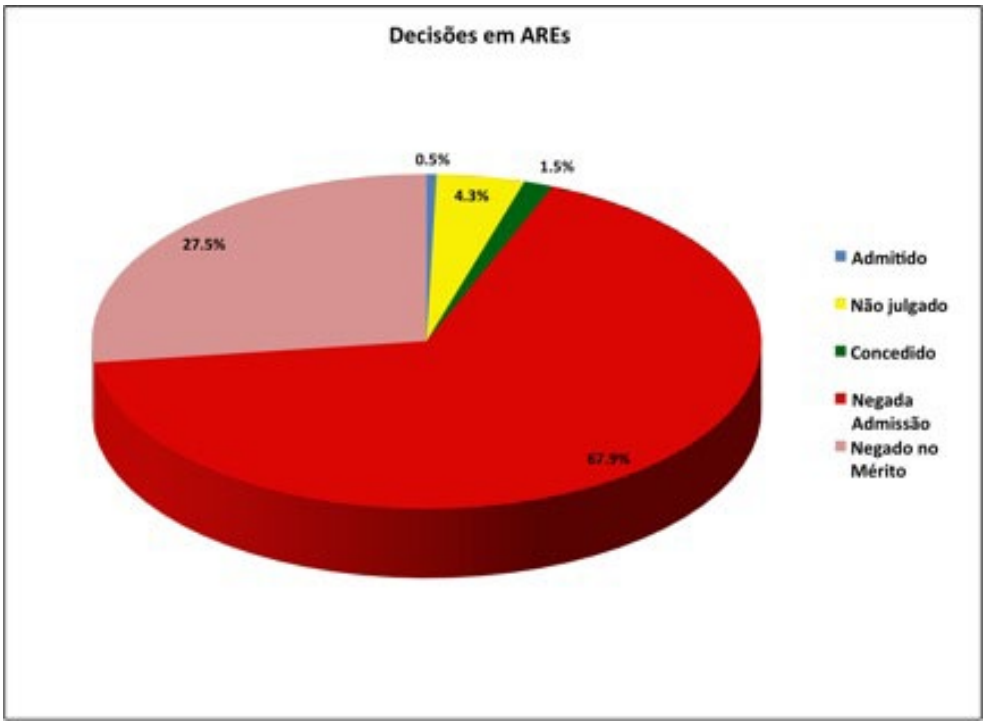


Enquanto que os 10 maiores litigantes são parte recorrente em 18,7% dos AREs autuados, eles concentram 16,7% dos AREs distribuídos pela Presidência do Supremo. A variação entre a concentração por parte dos 100 maiores litigantes nos processos autuados e distribuídos é quase nula: de 30,2% para 30,3%.

Por último, efetuamos o levantamento dos resultados das decisões tomadas pelo Supremo — seja pelos relatores, monocraticamente, seja pelas Turmas ou pelo Plenário, por meio de acórdão. Encontramos um total de 43.493 decisões em 44.741 AREs. Isso significa que alguns processos tiveram mais de uma decisão proferida. Um exemplo é quando há a decisão do relator ne-

gando admissão e a decisão do colegiado sobre o recurso contra tal negativa de admissão. Apenas 1.248 decisões foram proferidas em processos que já tinham outra decisão.

Essas decisões foram classificadas em: "Admitido", quando se trata de mero exame de admissão, porém com sucesso; "Não Julgado", quando a decisão não trouxe um efetivo posicionamento do Supremo sobre a admissibilidade ou mérito do recurso, por exemplo, quando a decisão foi de mera homologação de desistência ou de prejudicialidade; "Concedido", quando a decisão foi de sucesso ou sucesso parcial no exame de mérito; "Negada Admissão", quando houve exame negativo de admissibilidade; e "Negado no Mérito", quando houve exame negativo de mérito. A distribuição consta no Gráfico 6.



Como pode ser visto, 1,5% das decisões foram de concessão ou concessão parcial. Isso significa que, na melhor das hipóteses, 1,5% dos AREs tiveram sucesso ao menos parcial em reverter a última decisão dada antes que o processo chegasse ao Supremo. É possível que esse número seja inclusive menor, já que alguns AREs podem ter tido uma primeira decisão positiva seguida de uma nova decisão positiva, revertendo a primeira.

4. Discussão dos resultados

A principal conquista da EC 45 para o Supremo está gravemente ameaçada. Isso fica evidenciado por diversos resultados: o crescimento do número de AREs autuados; o crescimento do passivo de AREs não finalizados; o

crescimento, pela primeira vez em seis anos, do número de todos os processos distribuídos anualmente no Supremo.

Por outro lado, variação dos assuntos de AREs autuados em relação aos distribuídos mostra que a Presidência do Tribunal está de fato realizando um filtro. Se esse filtro fosse padronizado, como por exemplo, aceitar x% de todos os AREs de cada assunto, os resultados seriam muito diferentes daqueles encontrados. De fato, o Supremo claramente filtra muito mais os AREs sobre Direito do Consumidor do que aqueles sobre Direito Eleitoral. Filtra muito mais os AREs sobre Direito Civil do que aqueles sobre Servidor Público.

Mas se a Presidência do Tribunal está realmente filtrando mediante o critério da repercussão geral, porque está distribuindo tantos recursos? É absolutamente inviável que o direito brasileiro do consumidor, mesmo em toda sua complexidade, consiga gerar 3.611 controvérsias jurídicas (não fáticas, por óbvio) que nunca tenham sido admitidas para análise ou até decididas pelo Supremo. Isso em apenas 30 meses. O mesmo pode ser dito sobre as 4.691 novas questões de Direito Processual trabalhista e civil. Seriam realmente todas elas novas e nacionalmente relevantes? Um indício da resposta pode ser encontrado nos dados do *Relatório Supremo em Números — O Supremo e a Federação entre 2010 e 2012*,[10] que apontam que a cultura de recursos repetitivos ainda não foi vencida. Apesar de diminuir anualmente desde 2006, a proporção de processos dos dez maiores litigantes ainda era de 42% de todos os casos autuados no Supremo em 2012.

Os dados sobre AREs mostram um nível menor de concentração, embora ainda alto. Os 10 maiores autores respondem por quase 1 em cada 6 AREs. Mais importante ainda é a variação — ou ausência dela. Aqui mostra-se mais um indício de falta de filtragem pelo critério do ineditismo da questão jurídica. Se os AREs repetitivos estão sendo devolvidos pela Presidência do Supremo, seria de se esperar que os grandes litigantes diminuíssem sua concentração de processos. Não é realista afirmar que a Oi sozinha tenha levado 3776 novas questões de direito para o exame do Supremo. É por isso que apenas 190 desses AREs foram distribuídos. Ainda assim, um número alto de questões jurídicas inéditas e de impacto nacional.

Mas, embora os AREs de empresas privadas sejam razoavelmente filtrados, aqueles levados pelo poder público parecem ser considerados "inéditos" com grande freqüencia. A União teve cerca de mil dos seus 3490 AREs barrados. Ainda assim, são 2438 novas questões de direito distribuídas aos ministros do Supremo. No todo, fica claro que a concentração de muitos recursos repetitivos por parte de alguns poucos litigantes não é alterada pelo filtro da repercussão geral. Os 100 maiores continuam concentrando um terço dos AREs mesmo após um crivo que deveria produzir uma pulverização dos litigantes ao eliminar os recursos repetitivos.

[10] FALCÃO, Joaquim; ABRAMOVAY, Pedro; LEAL, Fernando; HARTMANN, Ivar A. *Relatório Supremo em Números. O Supremo e a Federação entre 2010 e 2012*. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2013. [no prelo]

Por fim, é espantosa a taxa de sucesso de um tipo de processo que ameaça paralisar o Tribunal em um futuro tão próximo. Nenhum mecanismo de revisão de decisões que protele a finalização de tantos processos, usando a estrutura da mais alta Corte do país, merece continuar existindo quando gera qualquer efeito em menos de 1,5% dos casos. Mais que isso, a possibilidade de recurso prevista no Código de Processo Civil contra a decisão do relator que não admite um ARE mostra-se excessiva e, na melhor das hipóteses, serve apenas a quem deseja prolongar a espera até a decisão final de processos que já receberam três outros julgamentos.

5. Conclusão

Reformas processuais sem embasamento em estudos estatísticos de viabilidade institucional e de sustentabilidade administrativa dos tribunais sempre foram a regra no Direito brasileiro. A última grande tentativa de transformar o Supremo em uma corte constitucional minimamente viável, a EC 45, até agora falhou.

O Congresso Nacional decide atualmente sobre o novo Código de Processo Civil — sem qualquer estudo empírico quantitativo que subsidie suas escolhas. A história se repete e o Judiciário brasileiro continua à mercê de decisões institucionais plenamente arbitrárias. Esse é o completo oposto daquilo preconizado pela Constituição de 1988: enquanto o Judiciário continuar falhando em entregar a prestação jurisdicional em tempo minimamente hábil, todos os direitos fundamentais dos brasileiros restam desprotegidos face às mais banais violações.

Bibliografia Adicional

KATZ, Daniel Martin. Quantitative Legal Prediction — or — How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry. Emory Law Journal, Vol. 62, 2013. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2187752

FALCÃO, Joaquim; ABRAMOVAY, Pedro; LEAL, Fernando; HARTMANN, Ivar A. II Relatório Supremo em Números. O Supremo e a Federação. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2013.

FALCÃO, Joaquim; CERDEIRA, Pablo; ARGUELHES, Diego Werneck. I Relatório Supremo em Números. O Múltiplo Supremo. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2011.

BIBLIOGRAFIA

ALENCAR, Marcelo Sampaio de. Engenharia de Redes de Computadores. São Paulo: Erica, 2012.

ALMEIDA FILHO, José Carlos de Araújo. Processo eletrônico e teoria geral do processo eletrônico: a informatização judicial no Brasil. 4. ed., rev. e atual. Rio de Janeiro: Forense, 2012.

BALKIN, Jack. Digital speech and democratic culture: a theory of freedom of expression for the information society. New York University Law Review. V. 79, n. 1, p. 1-58. abr 2004.

BELL, Daniel. The social framework of the information society. in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

BERG, Terrence. www.wildwest.gov: The impact of the Internet on state power to enforce the law. Brigham Young University Law Review, 2000.

BLUM, Renato M. S. Opice; ABRUSIO, Juliana Cunha (Coords.) Manual de direito eletrônico e internet. São Paulo: Lex, 2006.

BOYD, Danah. MARWICK, Alice. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128

BURK, Dan L. Federalism in Cyberspace. Connecticut Law Review, 28, 1996.

CASTELLS, Manuel. Infomationalism, Networks, and the Network Society: A Theoretical Blueprint. In: CASTELLS, Manuel (Org.). The network society: a cross-cultural perspective. Cheltenham: Edward Elgar, 2004.

CAVELTY, Myriam Dunn. Is anything ever new? Exploring the specificities of security and governance in the information age. in: DUNN CAVELTY, Myriam (Org.). Power and security in the information age: investigating the role of the state in cyberspace. Aldershot: Ashgate, 2007.

CLEMENTINO, Edilberto Barbosa. Processo judicial eletrônico: o uso da via eletrônica na comunicação de atos e tramitação de documentos processuais sob o enfoque histórico e principiológico, em conformidade com a Lei 11.419, de 19.12.2006. Curitiba: Juruá, 2007.

COMER, Douglas E. Computer Networks and Internets. 5a ed. Prentice Hall, 2008.

COTTER, Thomas F. Memes and Copyright. Tulane Law Review, Vol. 80, 2005. Disponível em:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=826465

DAHLGREN, Peter. The Internet, public spheres, and political communication. Dispersion and deliberation. in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

DALY, Angela. FARRAND, Benjamin. Scarlet v SABAM: Evidence of an Emerging Backlash Against Corporate Copyrights Lobbies in Europe? Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2095295

Decisão Capitol Records v. ReDigi:
http://www.wired.com/images_blogs/threatlevel/2012/02/redigiruling1.pdf

DIMAGGIO, Paul; HARGITTAI, Eszter; NEUMAN, W. Russell; ROBINSON, John P. Social implications of the internet. in: MANSELL, Robin (Org.). The information society. v. IV (Everyday life). New York: Routledge, 2009.

DIMOULIS, Dimitri. O direito de ofender: sobre os limites da liberdade de expressão artística. Revista Brasileira de Estudos Constitucionais — RBEC, v. 3, n. 10, p. 49-65, abr./jun. 2009.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

FALCÃO, Joaquim; ABRAMOVAY, Pedro; LEAL, Fernando; HARTMANN, Ivar A. II Relatório Supremo em Números. O Supremo e a Federação. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2013.

FALCÃO, Joaquim; CERDEIRA, Pablo; ARGUELHES, Diego Werneck. I Relatório Supremo em Números. O Múltiplo Supremo. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2011.

FARIS, Robert; ETLING, Bruce. Madison and the Smart Mob: The Promise and Limitations of the Internet for Democracy. The Fletcher Forum of World Affairs, 32, 2008.

FERREIRA, Ana Amelia Castro. Sistemas Tecnológicos e o Poder Judiciário. Racionalização ou Democratização da Justiça? Revista de Derecho Informático. no. 85, ago-2005.

FINKELSTEIN, M. E.. Direito do Comércio Eletrônico. 2a.. ed. Rio de Janeiro: Ed. Campus Elsevier, 2010.

FISHKIN, James. Possibilidades democráticas virtuais: Perspectivas da democracia via internet. In: EISENBERG, José; CEPIK, Marco. Internet e política: teoria e prática da democracia eletrônica. Belo Horizonte: UFMG, 2002.

FROOMKIN, A. Michael. Habermas@discourse.net: Toward a critical theory of cyberspace. Harvard Law Review, 116, 2003.

GASSER, Urs. PALFREY Jr., John G. Catch-As-Catch-Can: A Case Note on Grokster. Research Publication No. 2005 — October 2005. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=869030.

GRIMMELMANN, James. Saving Facebook. Iowa Law Review, Vol. 94, p. 1137, 2009. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262822

GRIMMELMANN, James. Some Skepticism About Search Neutrality. THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET, p. 435, Berin Szoka & Adam Marcus, eds., TechFreedom, January 2011. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1742444

HARTMANN, I. A. M.. Ciberdemocracia: A Personalidade Digital e A Motivação para o Engajamento Cívico na Internet. Revista de Direito das Novas Tecnologias, v. 8, p. 67, 2012.

HARTMANN, Ivar A. M. A Right to Free Internet? On Social Rights and Internet Access. Journal of High Technology Law, vol. XIII, n. 2, 2013.

HARTMANN, Ivar A. M. e-codemocracia: A Proteção do Meio Ambiente no Ciberespaço. Porto Alegre: Livraria do Advogado, 2010.

INTRONA, Lucas D. NISSENBAUM, Helen. Shaping The Web: Why The Politics Of Search Engines Matters. Information Society, Vol. 16, No. 3. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222009

JOHNSON, David R.; POST, David. Law And Borders — The Rise of Law in Cyberspace. Stanford Law Review, 48, 1995.

KATZ, Daniel Martin. Quantitative Legal Prediction — or — How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry. Emory Law Journal, Vol. 62, 2013. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2187752

KLEINWÄCHTER, Wolfgang. Internet co-governance. Towards a multilayer multiplayer mechanism of consultation, coordination and cooperation (M3C3). in: MANSELL, Robin (Org.). The information society. v. III (Democracy, governance and regulation). New York: Routledge, 2009.

KLOEPFER, Michael. Informationszugangsfreiheit und Datenschutz: Zwei Säulen des Rechts der Informationsgesellschaft. DöV. V. 6, 2003.

KUGELMANN, Dieter. Informationsfreiheit als Element moderner Staatlichkeit. DöV. v. 20, 2005.

LAZZARI, João Batista. O processo eletrônico como solução para a morosidade do Judiciário. Revista de previdência social. v.30, n.304, p.173-174, mar., 2006.

LEMLEY, Mark A.; LESSIG, Lawrence. The end of end-to-end: Preserving the architecture of the Internet in the broadband era. UCLA Law Review, 48, 2000.

LEMOS, Ronaldo ; Branco, S.. COPYLEFT, SOFTWARE LIVRE E CREATIVE COMMONS: A Nova Feição dos Direitos Autorais e as Obras Colaborativas. Revista de Direito Administrativo, v. 243, p. 180-210, 2006

LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. 1. ed. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, Marcel. Tutela e privacidade na Internet. 1. ed. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. Code. Version 2.0. New York: Basic Books, 2006.

LESSIG, Lawrence. The New Chicago School. The Journal of Legal Studies, n. 27, 1998.

LICOPPE, Christian; SMOREDA, Zbigniew. Rhythms and ties. Toward a pragmatics of technologically mediated sociability. in: KRAUT, Robert; BRYNIN, Malcolm; KIESLER, Sara (Orgs.). Computers, phones, and the internet: domesticating information technology. Oxford: Oxford Univ. Press, 2006.

LIMBERGER, Têmis. A informática e a proteção à intimidade. Revista da AJURIS. Porto Alegre, n. 80, p. 319-333, dez. 2000.

MAÑAS, José Luis Piñar. El derecho fundamental a la protección de datos personales. In: MAÑAS, José Luis Piñar (org). Protección de datos de carácter personal en Iberoamérica. Valencia: Tirant lo Blanch, 2005.

MAÑAS, José Luis Piñar. Proteccion de Datos: Origen, Situacion Actual y Retos de Futuro. Anais do Seminario de Derecho y Jurisprudencia. Madri, 2008. Disponível em: http://www.fcje.org.es/wp-content/uploads/file/jornada15/2_PINAR_1.pdf.

MEYER-PFLUG, Samantha Ribeiro. Liberdade de expressão e discurso do ódio: racismo, discriminação, preconceito, pornografia, financiamento público das atividades artísticas das campanhas eleitorais. São Paulo: Revista dos Tribunais, 2009.

MIRAGEM, Bruno. Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. Revista de Direito do Consumidor. N. 70. p. 41. São Paulo: Revista dos Tribunais, 2009.

MOREIRA, Renato de Castro. O Direito à liberdade informática. Revista da AJURIS. Porto Alegre, p. 139-167, dez. 1999.

NISSEMBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy. n. 17, 1998. Disponível em: http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf

O'ROURKE, Maureen A. Fencing Cyberspace: Drawing Borders in a Virtual World. Minnesota Law Review, 82, 1997.

OWEN, Bruce M. The Net Neutrality Debate: Twenty Five Years after United States v. AT&T and 120 Years after the Act to Regulate Commerce. Stanford Institute for Economic Policy Research. Discussion Paper No. 0615.

PASQUALE III, Frank. BRACHA, Oren. Federal Search Commission? Access, Fairness and Accountability in the Law of Search. Cornell Law Review, September 2008. Disponível em:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002453

REIDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. Texas Law Review, 76, 1998.

RHEINGOLD, Howard. The virtual community: homesteading on the electronic frontier. Cambridge (MA): The MIT Press, 2000.

RIBEIRO, Marcello Peixoto. Redes de Telecomunicações e Teleinformática. Rio de Janeiro: Interciência: 2012.

ROHRMANN, Carlos Alberto. Curso de direito virtual. Belo Horizonte: Del Rey, 2005.

ROSENBERG, Richard S. The social impact of computers. 3a. ed. Amsterdam: Elsevier Acad. Press, 2004.

SANTOS, Gustavo Ferreira. Da liberdade de expressão ao direito à comunicação. Direitos Fundamentais & Justiça, v. 10, p. 200-204, 2010.

SCHWABACH, Aaron. Reclaiming Copyright From the Outside In: What the Downfall Hitler Meme Means for Transformative Works, Fair Use, and Parody. Buffalo Intellectual Property Law Journal, 2012. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2040538

SILVA JUNIOR, Ronaldo Lemos da ; SOUZA, Carlos Affonso Pereira de ; BRANCO, Sergio. 'Responsabilidade Civil da Internet: uma breve reflexão sobre a experiência brasileira e norte-americana'. Revista de Direito das Comunicações, v. 1, p. 80-98, 2010.

SOUZA, Carlos Affonso Pereira de. Compartilhamento, Colaboração e Pirataria: questionamentos atuais sobre direito autoral. Revista Forense (Impresso), v. 383, p. 31-46, 2006.

WEBSTER, Frank. Theories of the information society. 2a. ed. London: Routledge, 2003.

WU, Tim. When code isn't law. Virginia Law Review, 89, 2003.

ZITTRAIN, Jonathan. The Future of the Internet and How to Stop It. New Haven: Yale University Press, 2008.

IVAR A. HARTMANN
Professor Assistente da FGV Direito Rio. Doutorando em Direito pela Universidade do Estado do Rio de Janeiro. Mestre em Direito Público pela PUC-RS. Mestre em Direito (LL.M.) pela Harvard Law School.

FICHA TÉCNICA

Fundação Getulio Vargas

Carlos Ivan Simonsen Leal
PRESIDENTE

FGV DIREITO RIO

Joaquim Falcão
DIRETOR

Sérgio Guerra
VICE-DIRETOR DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO

Rodrigo Vianna
VICE-DIRETOR ADMINISTRATIVO

Thiago Bottino do Amaral
COORDENADOR DA GRADUAÇÃO

André Pacheco Teixeira Mendes
COORDENADOR DO NÚCLEO DE PRÁTICA JURÍDICA

Cristina Nacif Alves
COORDENADORA DE ENSINO

Marília Araújo
COORDENADORA EXECUTIVA DA GRADUAÇÃO

Paula Spieler
COORDENADORA DE ATIVIDADES COMPLEMENTARES E DE RELAÇÕES INSTITUCIONAIS