Le nuove frontiere del documento informatico e della firma elettronica: dalla firma digitale attraverso quella grafometrica fino alla "mobile signature"

Andrea Lisi
Presidente ANORC – Associazione Nazionale Operatori e Responsabili della Conservazione digitale dei documenti
Coordinatore Digital&Law Department Studio Legale Lisi
Docente DMA e MIS Academy SDA Bocconi

^^^

Da tempo abbiamo poggiato, forse senza esserne del tutto consapevoli, i nostri documenti e i nostri contratti lungo i binari infiniti del web 2.0. E le certezze del diritto sembrano essere messe a dura prova dai confini incerti di nuove consuetudini che mutano spesso direzione proprio perché si muovono attraverso l'utilizzo di tecnologie digitali che si cambiano d'abito ogni giorno.
In verità la normativa, a partire dagli anni '90, sta provando (e a volte ci riesce anche bene) a inseguire queste continue trasformazioni che sono culturali, sociologiche, economiche, prima ancora che giuridiche. Ma sarà soprattutto l'opera di puntigliosa rilettura e interpretazione del giurista attento a questi mutamenti a permettere al diritto di evolversi e a far seguire una strada giuridicamente corretta a comportamenti contrattuali e documenti che sono ormai "privi di peso".
Per cercare di comprendere appieno le problematiche della firma di un documento informatico occorre prima di tutto capire cosa caratterizza il nuovo modo di documentare digitalmente fatti e atti giuridicamente rilevanti. Infatti, in modo inesorabile, ogni nostro comportamento avviene oggi on line e la nostra memoria non è più conservata su supporti che segnano in modo immodificabile il tempo di ogni nostra azione.
Possiamo dire oggi di possedere la prova informatica certa e inconfutabile del nostro acquisto su un sito di e-commerce? Riceviamo un'attestazione documentata e producibile in giudizio dalle procedure di home banking attraverso le quali effettuiamo un pagamento? Ha valore giuridico il contratto stampato che mi consegna un albergo dopo che ho siglato su un tablet la mia volontà di accettare le condizioni generali relative al mio pernotto?
Muoviamo i nostri passi lungo le strade della semplicità e della semplificazione telematica, senza neppure porci quelle domande che invece ci appaiono ovvie nel vecchio mondo garantito dalla carta sottoscritta. In verità, siamo letteralmente travolti da questo passaggio epocale che ci porta a dimenticare le ragioni del documento pesante e statico che ci aveva abituati a testimoniare con certezza le nostre azioni giuridicamente rilevanti per cedere il passo a un documento dinamico, che si condivide, che diventa "partecipativo", ma che anche si modifica ogni giorno e non sempre garantisce una memoria autentica delle nostre azioni passate.

Cos'è un documento informatico?

Secondo l'art. 1, comma 1°, lett. p) del Codice dell'amministrazione digitale (C.A.D. – contenuto nel Decreto Legislativo 82/2005, come modificato recentemente dal D. Lgs. 235/2010) per documento informatico deve intendersi la "**rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti**". Ancora più in particolare, il Decreto del Ministero Economia e Finanze del 23 gennaio 2004 (contenente le *modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto*) specifica che il documento digitale è costituito da "testi, immagini, dati strutturati, disegni, programmi, filmati formati tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica, di cui sia identificabile l'origine". Quindi, **nel mondo del web 2.0 il documento non è solo un .pdf** (che in modo rassicurante ci ricorda l'immagine digitalizzata di un foglio di carta), **ma è qualsiasi dato digitale giuridicamente rilevante e strategico per l'impresa o la PA:** un tracciato EDI, un log file generato da una transazione commerciale su un sito web, una comunicazione e-mail, un'analisi di dati di navigazione, un filmato digitale etc. Un documento di

questo tipo, che è "rivestito di bit", prescinde dal supporto per la sua sopravvivenza tanto che per poter essere garantito nel tempo deve essere riprodotto in tanti duplicati indistinguibili dall'originale (la copia di un bit, infatti, è esattamente identica al suo originale) e, quindi, riversato su diversi supporti informatici. Il problema è che se prima la carta (o qualsiasi altro supporto) garantivano l'immodificabilità al documento e, quindi, ne preservavano la sua autenticità, oggi un qualsiasi documento informatico è sempre soggetto a modifiche: come si fa, quindi, a garantirgli validità giuridica e sopravvivenza certa nel tempo?

Il documento informatico garantisce la forma scritta?

Il concetto di "forma scritta" va slegato dal concetto di firma elettronica. Nel diritto romano si affermava solennemente: "Verba volant, scripta manent" e "Quod non est in actis non est in mundo". Oggi, nell'ordinamento giuridico italiano, il concetto di forma scritta (sia nella normativa dedicata al commercio elettronico[1], sia nel diritto dei consumatori[2], ma anche nei principi del commercio internazionale[3]) è legato a una forma durevole e affidabile di comunicazione. Infatti, a che serve documentare? Non certo a conferire valore ad atti e fatti che sono nella maggior parte dei casi validi e giuridicamente rilevanti anche senza una specifica forma, ma a testimoniare con certezza ciò che è accaduto o è stato manifestato da qualcuno[4].

Il CAD, ai sensi dell'art. 20 comma 1bis, stabilisce che il documento informatico soddisfa i requisiti della forma scritta quando garantisce in modo oggettivo integrità, sicurezza e immodificabilità. Stessa cosa prevede l'art. 21 comma 1 per il documento informatico con firma elettronica semplice.

Occorre quindi prestare massima attenzione al formato utilizzato e al supporto informatico prescelto per salvaguardare il documento informatico. Per quanto riguarda il supporto, però, è necessario considerare non il singolo supporto fisico su cui il documento informatico è stato salvato, bensì occorre riferirsi all'intero sistema informatico di "conservazione" che, nell'insieme delle soluzioni tecnologiche prescelte, è in grado di garantire la qualità, l'integrità, la sicurezza e l'immodificabilità del documento informatico nel tempo.

Lo scopo della "forma scritta digitale" è quello, quindi, di ottenere garanzie circa l'integrità, la sicurezza e l'immodificabilità nel tempo di un documento, o meglio di un determinato "atto", "fatto" o "dato", in modo da consentirne la sua corretta documentazione.

Le nuove firme del web 2.0

Nel nostro ordinamento esistono oggi varie tipologie di firma elettronica. Per comprendere appieno la portata dell'ultima riforma contenuta nel CAD e le differenze di utilizzo e di valore probatorio delle varie tipologie di firma occorre aver ben chiaro cosa si intende per firma e sottoscrizione.

"Nel lessico usuale si fa una certa confusione tra firma e sottoscrizione talché, a prima vista, non è dato con chiarezza scindere i concetti afferenti ai due vocaboli. Giuridicamente, invece, le

[1] Si fa riferimento al D. Lgs. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno)

[2] Si fa riferimento, ad esempio, all'informativa "scritta" in favore del consumatore che deve essere garantita dalla possibilità di essere conservata. L'art. 53 del Codice del Consumo, infatti, specifica che "il consumatore deve ricevere conferma per iscritto o, a sua scelta, su altro supporto duraturo a sua disposizione ed a lui accessibile, di tutte le informazioni previste dall'articolo 52, comma 1, prima od al momento della esecuzione del contratto".

[3] Nell'art. 1.10 Definitions dei Principi UNIDROIT si legge testualmente: "in these Principles "writing" means any mode of communication that preserves a record of the information contained therein and is capable of being reproduced in tangible form". Quindi per "forma scritta" si intende qualsiasi forma di comunicazione che conservi la documentazione delle informazioni contenute e sia riproducibile in forma tangibile.

[4] Infatti, la forma scritta *ad substantiam* per il nostro ordinamento (basato sull'aformalismo contrattuale) è essenziale solo per alcuni atti e contratti (art. 1350 c.c. e altre fattispecie speciali previste dalla legge). Occorre, quindi, ben differenziare gli aspetti probatori della "forma scritta", da quelli più "formali", previsti per la validità ed esistenza dell'atto.

differenze sono anche sostanziali, sicché si potrebbe affermare che la sottoscrizione sta alla firma come la *species* al *genus*, come la parte al tutto […] sottoscrivere vuol dire scrivere sotto, ossia letteralmente scrivere sotto uno scritto, un documento, un foglio, una qualsiasi scrittura quasi a sigillare i medesimi con l'impronta dei segni alfabetici formanti il nome, inteso nella sua più ampia accezione" (Dott. A. Morello, Voce Sottoscrizione, Nuovissimo Digesto Italiano, Torino, 1957). La modernità di queste parole pur "scritte" ormai cinquant'anni fa è evidente, soprattutto perché attraverso le stesse si possono cogliere perfettamente anche le differenze tra forma scritta e scrittura privata con sottoscrizione autografa, tra firma elettronica e firma digitale, che tanto fanno discutere in questi giorni.

La sottoscrizione conferisce la paternità al documento cartaceo, è il suggello della sua appartenenza a un soggetto: su di essa si è sviluppata la tradizione giuridica dal diritto romano sino ad oggi. Per alcuni atti e contratti la "forma scritta sottoscritta" viene richiesta *ad substantiam*, per altri *ad probationem*, per altri ancora, più importanti, è necessario l'atto pubblico (ovvero è necessario suggellare l'atto in presenza di un notaio) che attesti incontrovertibilmente la sua provenienza e riconoscibilità. Ma **molti dei nostri contratti non si devono per forza perfezionare con la forma scritta e sottoscritta per risultare validi ed efficaci, ma si possono concludere anche attraverso manifestazioni tacite di volontà, comunque riconducibili ai soggetti contraenti**. Determinati comportamenti sono, quindi, giuridicamente riconducibili a un soggetto perché incompatibili con una volontà contraria e rendono quell'atto o quel contratto imputabile giuridicamente a quel soggetto perché in qualche modo esso lo ha "siglato": pur non avendolo sottoscritto quell'atto gli appartiene. Così accade per la maggior parte dei contratti che "stipuliamo" ogni giorno, a partire dall'acquisto di un giornale di prima mattina, con il semplice pagamento del prezzo di vendita![5] È chiaro che questi comportamenti giuridicamente rilevanti, in caso di contestazione, vanno provati e proprio per questo per i nostri affari più rilevanti si mira sempre a ottenere una documentazione certa e inoppugnabile di quanto accaduto.

Nel documento scritto e sottoscritto (scrittura privata con firma autografa) la sottoscrizione riversata sul foglio custodisce in modo immodificabile l'appartenenza di quella dichiarazione a colui che ha apposto la firma. Ma è il supporto che garantisce l'idonea documentazione nel tempo di quanto dichiarato e firmato.

Nel mondo digitale non ci sono supporti da incidere e non sono i supporti a garantire la conservazione nel tempo, solo determinati processi informatici possono sia garantire l'appartenenza di una dichiarazione resa in un ambiente informatico o di un comportamento digitale rilevante, sia preservarne l'integrità/autenticità nel tempo.

Ecco quindi che abbiamo nel nostro ordinamento quattro tipologie di firma elettronica (previste dall'art. 1 del CAD):

- **Firma elettronica semplice** (lett. q) - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
- **Firma elettronica avanzata** (lett. q-bis) - Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
- **Firma elettronica qualificata** (lett. r) - Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la

[5] E questo succede in tutti i siti di e-commerce dove la volontà di contrarre è inevitabilmente confermata dal pagamento con carta di credito!

creazione della firma

- **Firma digitale** (lett. s) - Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

Solo alla firma digitale e alla firma elettronica qualificata (in quanto *species* della firma elettronica avanzata) e alla stessa firma elettronica avanzata (ma con notevoli limiti[6]) viene garantita l'equivalenza con la "forma scritta e sottoscritta". Alla firma elettronica semplice viene, invece, garantito un valore giuridico che dipende dal processo in cui essa viene inserita e tale giudizio è rimesso alla libera valutazione di un giudice. Essa è stata pensata a livello comunitario proprio per regolamentare tutte quelle diverse e possibili transazioni commerciali elettroniche tipiche dei processi di e-commerce (si pensi alle negoziazioni on line garantite da pagamenti con carte di credito, fino alle ultime frontiere del pagamento con smart-phone[7])

In verità, se da una parte la firma digitale assolve *ex lege* alla funzione di garantire con certezza assoluta al documento informatico su cui è apposta imputabilità giuridica e forma scritta – dal momento che il processo tecnologico che ne è alla base è rigidamente regolamentato ed è reso sicuro dalla sussistenza di standard internazionali, ed essa è quindi affidabile *in re ipsa* - dall'altra parte sia la firma elettronica semplice sia la firma elettronica avanzata non si riferiscono a processi tecnologici rigidamente individuati, ma costituiscono il *genus* di infinite, possibili *species* di firma. La loro validità, quindi, dipende inevitabilmente dalle tecnologie utilizzate e dal contesto in cui sono inserite.

La firma elettronica avanzata

In verità l'inserimento recente nel nostro ordinamento della firma elettronica avanzata è stato reso molto "timido" nell'attuale Schema di DPCM ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, del D. L.gvo 7 marzo 2005 n. 82, che conterrà le nuove regole tecniche per le firme digitali ed elettroniche e che dovrebbe essere pubblicato a breve in Gazzetta Ufficiale. Infatti, in tale schema di DPCM si prevede all'art. 60 che la firma elettronica avanzata, realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che realizza la soluzione di firma o comunque se ne serve[8].

La firma elettronica semplice, ma soprattutto la firma elettronica avanzata, costituiscono processi tecnologici neutri che, se sono configurati in modo tale da garantire la paternità della manifestazione di volontà e l'integrità della documentazione digitale della stessa, allora assolvono a quelli che sono i requisiti richiesti dal nostro ordinamento e non possono che essere considerate prove informatiche producibili in giudizio e che garantiscono la "forma scritta".

---

[6] Limiti ricavabili essenzialmente, come vedremo, dalla lettura dello Schema di DPCM ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, del D. L.gvo 7 marzo 2005 n. 82 (la bozza è pubblicata sul sito di DigitPA).

[7] Importanti scenari si stanno aprendo grazie alla tecnologia RFID-NFC che si trova ormai nei dispositivi cellulari di ultima generazione e che è supportata dalle più conosciute piattaforme mondiali di carte di credito-debito che hanno abilitato metodi di pagamento tramite i nostri telefoni cellulari.

[8] Questa limitazione svuota di molto l'innovatività insita in questo processo di firma perché di fatto lo riporta nell'alveo delle forme convenzionali previste nel codice civile all'art. 1352 laddove già dal 1942 (anno di entrata in vigore del codice) si prevedeva che "se le parti hanno convenuto per iscritto di adottare una determinata forma per la futura conclusione di un contratto, si presume che la forma sia stata voluta per la validità di questo".

La firma elettronica avanzata, in particolare, non può (e non deve) essere ricondotta a un determinato software o a una determinata tecnologia, ma essa si riferisce genericamente a un qualsiasi sistema neutro, sicuro e affidabile che garantisca l'appartenenza di un documento informatico reso immodificabile a un determinato soggetto[9].

L'ultima frontiera della firma "grafometrica"

Nell'alveo della firma grafometrica possono ricondursi diversi processi. Noi soffermeremo la nostra attenzione soprattutto sulla firma biometrica grafometrica che presenta molti scenari di utilizzo e soprattutto una possibile solidità giuridica.

Esistono molti prodotti hardware, già sul mercato, che semplicemente digitalizzano la firma autografa acquisendone l'immagine nel momento in cui essa viene impressa dal sottoscrivente sullo schermo del tablet utilizzato per tale scopo. In questo caso, non vengono acquisiti dal sistema dei dati biometrici legati alla firma, ma semplicemente viene associata al documento informatico l'immagine della firma. Inutile dilungarsi su questo tipo di firma: essa non può che avere l'efficacia giuridica degli artt. 2712[10] cc e 2719[11] cc e, quindi, può essere facilmente disconosciuta[12].

Inoltre, la biometria grafometrica (come altre forme di biometria) può essere utilizzata come metodo di autenticazione informatica[13] e, quindi, anche per autorizzare l'utilizzo (in remoto) di certificati di firma digitale. In questo caso l'acquisizione da parte del tablet non è solo relativa all'immagine della propria firma, ma al dato comportamentale del soggetto sottoscrivente e tale acquisizione viene utilizzata come credenziale forte di autenticazione[14] per garantire un accesso riservato di transazione, ma anche come modello di sottoscrizione digitale e, quindi, assicurare un

---

[9] Secondo l'art. 56 dello Schema di Decreto contenente le Regole Tecniche già richiamato si precisa che: "le soluzioni di firma elettronica avanzata devono garantire:
a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
d) la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati".

[10] Art. 2712.
Riproduzioni meccaniche.
Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

[11] Art. 2719. Copie fotografiche di scrittura. (Le copie fotografiche di scritture hanno la stessa efficacia delle autentiche, se la loro conformità con l'originale è attestata da pubblico ufficiale competente ovvero non è espressamente disconosciuta).

[12] La sola immagine di una sottoscrizione, infatti, non portando con sé gli ulteriori elementi grafometrici tipici della "sottoscrizione su carta" rende di fatto impossibile un processo di verificazione.

[13] Secondo il Codice Privacy (D. Lgs. 196/2003) art. 4 comma 1 lett. c) e d) per **autenticazione informatica** deve intendersi "l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità" e per **credenziali di** autenticazione "i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica".

[14] Secondo l'allegato B) al Codice Privacy le credenziali di autenticazione possono consistere "in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave".

accesso in remoto al proprio certificato di firma (custodito ad esempio in un HSM[15]). L'utilizzo della firma grafometrica come credenziale forte di autenticazione pone delicati quesiti in termini di privacy, in quanto necessita della creazione di una banca dati con le firme biometriche in modo da consentirne ogni volta la verifica, rendendo quindi indispensabile una notifica del trattamento al Garante (ex art. 37 lett. a del Codice Privacy) e la proposizione di un interpello all'Autorità Garante ai sensi dell'art. 17 del Codice privacy il cui esito potrebbe non essere favorevole[16].

Infine, arriviamo alla firma biometrica grafometrica in senso stretto. Qui siamo di fronte alla trasposizione in ambiente digitale delle caratteristiche tipiche della firma autografa, in quanto il sistema consente di associare al documento (e tale associazione deve essere realizzata in modo sicuro, statico e immodificabile) il parametro biometrico della sottoscrizione (tipicamente: la velocità di scrittura, la pressione esercitata, l'angolo di inclinazione della penna, l'accelerazione dei movimenti e il numero di volte che la penna viene sollevata dalla carta), in modo da consentire una verifica ex post dell'autenticità della firma in caso di disconoscimento.

Questo tipo di firma può certamente essere sussumibile nel *genus* ampio della firma elettronica avanzata (se il processo garantisce l'identificazione del firmatario, un legame indissolubile con il documento informatico sottoscritto e la verifica dell'integrità dell'oggetto informatico composto dal documento + il dato biometrico della firma). Ma, in verità, questa tipologia di firma costituisce più propriamente una categoria a sé stante e deve ritenersi riconosciuta nell'ordinamento giuridico italiano proprio perché già prevista dal nostro codice civile: essa è semplicemente una firma autografa riversata non su un foglio di carta, ma associata indissolubilmente a un documento informatico, a patto che esso abbia i requisiti tipici previsti per garantire la forma scritta ai sensi dei già citati artt. 20 e 21 del CAD[17]. Quindi, pur con una specifica attenzione alle problematiche tipiche della corretta formazione del documento informatico, della corretta conservazione dell'oggetto informatico contenente documento e dati di firma biometrica e con una particolare considerazione alle delicate questioni di sicurezza e privacy che la protezione del dato biometrico comporta, possiamo affermare che la firma autografa digitale o grafometrica può trovare le ragioni giuridiche per una sua autonoma esistenza e validità nei principi generali del nostro ordinamento, anche a prescindere dalle Regole Tecniche sulle firme elettroniche in via di pubblicazione.

Per ulteriori approfondimenti potete scaricare l'e-book "Guida pratica su firme elettroniche e firme grafometriche" realizzato dal team del Digital & Law Department e pubblicato da Edisef al seguente link:

http://www.edisef.it/guida-pratica-su-firme-elettroniche-e-firme-grafometriche

[15] Gli HSM (hardware security module) sono dei dispositivi sicuri per la firma digitale massiva.

[16] Art. 17. Trattamento che presenta rischi specifici
1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

[17] La firma grafometrica viene richiamata anche nel CAD all'art. 25 comma 2 laddove si precisa che "l'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico".