

TAMPERING

Attività di contrasto a manipolazioni di sostanze alimentari a scopo terroristico.

PREMESSA.

Il presente intervento non ha alcuna pretesa di esaustività, assoluta scientificità o autorevolezza. Tanto meno nel caso di un argomento così sfuggente e poco esplorato. Non pretende nemmeno di fornire efficaci strumenti di contrasto ad un'insidia tra le più occulte ed odiose.

Vuole solo essere un contributo alla comprensione di un fenomeno per molti versi ancora oscuro e creare molti più dubbi di quanti ne possa risolvere.

Spesso, solo il dubbio consente la vittoria.

1. DEFINIZIONE, CLASSIFICAZIONE ED ENTITA' DEL FENOMENO.

Il termine "tampering" deriva dal verbo "to tamper", ossia "modificare qualcosa senza permesso, per lo più per provocare un danno"¹. In epoca recente, il vocabolo è stato utilizzato per definire una serie di comportamenti dolosi e fonte di pericolo in vari campi, da ultimo quello informatico, connessi alla manomissione di beni materiali o immateriali.

Non del tutto confacenti appaiono altre definizioni del vocabolo tentate nel tempo, come²: "contaminazione dolosa di un prodotto (o di un servizio) compiuta al fine di danneggiare il marchio dell'azienda produttrice". E' evidente che da tale definizione resterebbero escluse tutte le azioni non dirette allo scopo enucleato, che in realtà è solo uno di quelli possibili.

Non è il nostro scopo trovare una definizione semantica, per quanto sia rilevante avere una chiara idea dell'oggetto della discussione, sicché ci accontenteremo della pur vaga indicazione del semplice dizionario di lingua.

Ma la prima accezione del termine che abbia in qualche modo interessato il vasto mondo della sicurezza riguarda, appunto, la sofisticazione alimentare, e segnatamente quella operata a scopo di terrorismo, insorta tra gli anni settanta ed ottanta ad opera di gruppi eversivi operanti in ambito internazionale. Famoso è rimasto il caso di adulterazione dei pompelmi Jaffa, di produzione israeliana, da parte di terroristi palestinesi.

In tutti i casi, si tratta di azioni che consentono di ottenere effetti, psicologici prima ancora che concreti, molto incisivi a fronte di costi, rischi e difficoltà spesso assai contenuti. Molto spesso, poi, lo scopo è connesso più alla visibilità dell'evento che alle sue effettive conseguenze.

La frequenza del fenomeno è decisamente diversa dalla sua effettiva visibilità. Poiché, infatti, gli effetti sostanziali sono determinati dalla diffusione della notizia più che dai danni materiali che l'evento arreca, è tendenza comune da parte delle vittime mantenere il massimo riserbo sugli episodi di tampering se solo ciò sia possibile. E' quindi opinione universale degli analisti che le notizie che trapelano siano una sorta di punta dell'iceberg di un fenomeno assai meno

¹ Longman Dictionary.

² Dizionario di miaeconomia.it

infrequente di quanto si pensi. Ovviamente, trattandosi di un c.d. “numero oscuro”, l’entità effettiva dei fenomeni di tampering è oggetto di valutazioni prudenziali. In questa sede, quindi, ritengo che sia di scarso interesse scientifico cercare di determinare un numero che, di per sé, non avrebbe alcun significato, anche e soprattutto perché riferito a Paesi diversi dal nostro.

In estrema sintesi, si tratta di un atto di sabotaggio di natura assai peculiare, che possiamo classificare fondamentalmente in base agli autori ed in base alle merci interessate, anche alla luce dei fini perseguiti con gli attacchi.

In relazione ai soggetti agenti, possiamo distinguere atti riferibili a:

- elementi affetti da turbe psichiche (vds. Unabomber), che agiscono per le ragioni più disparate;
- dipendenti dell’organizzazione colpita, animati da desiderio di rivalse o di vendetta;
- terroristi, generalmente di matrice etnica o ideologica, con particolare riferimento –nel recente periodo- ad animalisti e pacifisti;
- criminali comuni, che agiscono a scopo di estorsione o ricatto ovvero per conto di soggetti economici concorrenti della vittima;
- agenti di potenze straniere, che compiono atti tattici ispirati da scopi strategici.

Con riferimento ai prodotti interessati dall’adulterazione, fondamentale è lo scopo che gli autori si prefiggono, essendo diversi sia l’estensione che la gravità degli effetti proprio in relazione ai beni colpiti, oltre che alle modalità di azione. In via generale, possiamo distinguere:

- materie prime industriali e semilavorati;
- prodotti coltivati in sede di produzione;
- prodotti alimentari deperibilissimi;
- altri prodotti alimentari;
- prodotti farmaceutici, parafarmaceutici e cosmetici;
- generi non food (in tal caso, spesso si tratta non di sofisticazione in senso stretto ma di manomissione tale da renderli pericolosi).

Non è detto che le azioni criminali comprendano una sola categoria di beni. Si pensi al caso in cui lo scopo sia quello di colpire un paese produttore o una multinazionale operante in più settori.

In questa sede, limiteremo le nostre considerazioni ai prodotti alimentari.

Quanto alla fase del ciclo di produzione o della supply chain nella quale l’azione si compie, la complessità delle dinamiche economico-distributive dell’attuale società ha l’effetto di rendere viepiù complesse le possibili problematiche, quand’anche ciò non significhi una maggior facilità di aggressione. Anche il sempre maggior uso di cibi preparati commercialmente (cibi pronti da cuocere e precotti in particolare) rientra in tale valutazione, essendo logico che l’uso di materie prime per confezionare il cibo in casa sia intrinsecamente più sicuro. Ciò anche in considerazione del fatto che i cibi preconfezionati sono spesso prodotti da aziende di notevoli dimensioni facenti capo a multinazionali del settore, che sono nel mirino di molte organizzazioni ostili.

Quanto più a monte avviene il tampering, tanto più estese saranno le conseguenze. E’ intuitivo che un’aggressione condotta su materie prime e semilavorati determinerà la contaminazione di un elevato numero di referenze, anche di tipologie assai diverse e facenti capo a diversi marchi. In tal caso, quindi, non sarà ipotizzabile un’azione condotta contro un’azienda specifica –a meno che non si tratti del produttore medesimo, il che sarebbe improbabile- mentre sarà maggiormente probabile, per esempio, un’aggressione terroristica o condotta per scopi di “guerra”.

Sulla misura in cui, invece, tale complessità influisca sulle possibilità di azione criminale, le opinioni divergono. Lester Crawford, Deputy Commissioner della FDA (Food and Drug Administration), sostiene che l'ampiezza dei volumi, la moltitudine delle origini dei beni e la lunghezza e complessità delle linee di logistiche incrementino notevolmente i rischi di contaminazione. Non mancano tuttavia i sostenitori del fatto che proprio le complessità evidenziate abbiano reso i processi produttivi e distributivi più controllati e controllabili, e quindi più sicuri che nel passato.

Entrambe le tesi hanno indubbiamente elementi di forza e punti deboli, sui quali non appare opportuno concentrarsi in questa sede. Ciò anche perché la scelta degli obiettivi cadrà sempre su prodotti materialmente avvicinabili da parte degli agenti, o perché di per sé aggredibili (p.es. prodotti esposti in vendita) o perché raggiungibili per circostanze particolari (si pensi al caso di attivisti infiltrati o reclutati).

E' indubbio, invece, che il progresso tecnico-scientifico consenta di fatto una grande scelta in materia di agenti contaminanti. Una ricerca svolta nel 2002 ha censito un numero di agenti patogeni potenzialmente presenti nelle sole sostanze alimentari ben cinque volte superiore al numero di quelli noti 50 anni fa¹. Tale incremento non solo moltiplica i possibili inquinanti ma rende estremamente flessibili le tecniche di contaminazione, adattandole a tutta la possibile gamma di bersagli. Per esempio, è oggi possibile risolvere le problematiche connesse alla sopravvivenza in attività degli agenti patogeni in relazione alle temperature di conservazione, di cottura o alla composizione delle atmosfere modificate di confezionamento dei prodotti alimentari deperibili.

NOTA.

Nell'esposizione che segue, faremo molto spesso riferimento agli Stati Uniti d'America. Ciò non è dovuto a sudditanza culturale (peraltro assolutamente ingiustificata da parte nostra) ma al semplice fatto che si tratta di un Paese assolutamente all'avanguardia nel settore specifico, sia in termini di studi effettuati e di dati disponibili che in termini di legislazione e predisposizioni organizzative. Esso costituisce, quindi, un case study particolarmente interessante, a prescindere da ogni altra considerazione. E' bene, comunque, precisare che - da un punto di vista concreto - è l'Italia il paese al mondo nel quale la sicurezza alimentare è più tutelata e garantita.

In tema di attualità ed entità della minaccia, essendo gli USA uno dei Paesi esposti a maggior rischio terroristico, ci limiteremo ad osservarne l'atteggiamento recente nei confronti del problema specifico:

- negli ultimi 15 mesi sono stati arruolati dalla FDA 600 addetti in più, 400 dei quali adibiti a controlli sull'importazione di sostanze alimentari, con una spesa espressamente dedicata al contrasto del tampering di 151 milioni di \$, finalizzata alla "prevenzione, deterrenza e capacità di risposta alla minaccia bioterroristica";
- l'8 febbraio 2002, l'FBI ha stipulato un accordo con il Food Marketing Institute in base al quale l'ISAC (Food Industry Security and Analysis Center) si occupa dello scambio informativo tra il governo federale e l'industria alimentare in materia di tampering. Le informazioni oggetto di analisi ed interscambio non riguardano solo la sofisticazione alimentare ma anche la protezione fisica delle industrie e la sicurezza delle infrastrutture informatiche. Il National Infrastructure Protection Center dell'FBI ha annunciato di avere in

¹ Fonte: Dipartimento della Salute USA.

corso analoghi accordi con le organizzazioni elettriche, bancarie, finanziarie, di telecomunicazione e di approvvigionamento idrico;

- il 12 giugno 2002 è stato promulgato il Public Health Security and Bioterrorism Preparedness and Response Act, meglio noto come “Bioterrorism Act”. Su cinque titoli che compongono la legge, due sono dedicati al cibo ed all’acqua potabile;
- il 21 marzo 2003 sono state pubblicate, congiuntamente dal Dipartimento della salute, FDA e Center for Food Safety and Applied Nutrition, quattro “guide per l’industria”, rispettivamente dedicate alla prevenzione e sicurezza di:
 1. distribuzione alimentare e ristorazione;
 2. industria e trasporto di cosmetici;
 3. industria e trasporto alimentare;
 4. importazione e filiere alimentari.

Tutti questi segnali di attenzione non possono che costituire l’indubbia prova –qualora ve ne fosse bisogno- di quanto il problema sia sentito e preoccupi gli organismi federali americani. E’ evidente che uno sforzo organizzativo, concettuale ed economico di queste dimensioni derivi anche da concreti segnali di esposizione a pericolo, con ogni probabilità derivanti anche da informazioni e valutazioni compiute dalle agenzie di sicurezza federali.

L’attenzione con la quale si guarda al settore specifico nasce, peraltro, anche da ulteriori considerazioni. Annualmente negli USA si registrano 76 milioni di casi di infermità “foodborne” (ossia originate in ambito alimentare) con 325.000 ospedalizzazioni, 5.000 decessi ed un impatto economico stimato in alcuni miliardi di \$.¹ A prescindere dalla minaccia terroristica, dunque, un tale stato di cose evidenzia l’estrema vulnerabilità della società occidentale in materia di sicurezza alimentare.

2. IMPATTO DELLE AZIONI DI TAMPERING.

Dalla semplice esposizione di queste considerazioni, appare evidente che ci si trovi di fronte ad un problema reale, le cui conseguenze sarebbero devastanti non solo sulla salute pubblica ma anche su settori determinanti per l’economia occidentale –ed europea in particolare- e sulla psiche individuale e collettiva.

L’impatto del tampering, infatti, trascende di gran lunga quello “normale” dovuto ad un’azione terroristica.

Di per sé, il terrorismo ha per scopo la creazione di uno stato di paura e di insicurezza diffusa, mantenendo un aggregato sociale ostaggio del rischio di attacco o distruzione. Si tratta, quindi, di attività criminali espressamente rivolte a colpire la psicologia, individuale e collettiva, di un target di individui determinati.

In estrema sintesi, il terrorismo è una forma di psicologia applicata.

Orbene, l’effetto psicologico è strettamente connesso alla rilevanza conscia ed inconscia di ciò che viene colpito dall’azione. Nel terrorismo “classico”, distinguiamo tra azioni mirate a persone/oggetti simbolici e azioni condotte in modo indiscriminato: notiamo immediatamente che gli effetti sono molto più devastanti nel secondo caso, in quanto investono la necessità di sicurezza che è al secondo livello della nota piramide di Maslow. Ma ricordiamo che al primo livello della piramide c’è la sussistenza, e la sussistenza è determinata dall’alimentazione. Ciò che colpisce la nostra possibilità di sopravvivenza fisica basilare, quindi, colpisce la radice stessa del nostro sistema di

¹ Fonte: Center for Disease Control and Prevention

bisogni elementari, ed ha quindi un impatto devastante sulla nostra psiche, agendo sugli istinti fondamentali.

E questo è esattamente lo scopo che il terrorista si prefigge con il tampering.¹

Vi sono ,poi, gli impatti di natura economica, che possono essere limitati alla specifica azienda bersaglio dell'azione di tampering ovvero interessare un intero sistema economico, sia come obiettivo dell'attacco che per la rilevanza economico-finanziaria dell'azienda colpita.

Particolarmente rilevanti potrebbero essere i danni per l'economia europea, e segnatamente per i paesi del Mediterraneo, per i quali da un lato l'industria alimentare assume dimensioni di grande rilievo e dall'altro il mercato alimentare è particolarmente evoluto, importante e vicino ai consumatori. Esso, inoltre, è caratterizzato da una grande frammentazione di offerta e di domanda nonché da un'elevata componente di localismi. Vi sono quindi prodotti dei quali un episodio di tampering potrebbe addirittura comportare l'estinzione.

Nella valutazione dei danni all'impresa vanno ricompresi, ovviamente, sia il danno emergente che il lucro cessante, sintetizzabili come segue:

- spese connesse alle analisi di laboratorio;
- spese di recall e stoccaggio;
- costi di gestione connessi al ciclo delle merci;
- spese legali;
- risarcimenti;
- costi assicurativi;
- costi derivanti dalla necessità di comunicazione;
- eventuali costi connessi alla chiusura, temporanea o definitiva, di esercizi commerciali o produttivi o di strutture logistiche²;
- spese di smaltimento e decontaminazione;
- decremento delle vendite, che può giungere fino al completo azzeramento³;
- effetto di medio termine sulla fiducia del consumatore/cliente, con conseguente riduzione della produzione/vendita;
- costi di rilancio del prodotto e dell'azienda;
- diminuzione del flusso finanziario;
- mancati incassi.

E' del tutto ovvio che nel caso di aggressione rivolta ad un intero sistema aziendale o addirittura ad una nazione, le conseguenze economiche non siano la semplice somma algebrica dei danni subiti dalle singole aziende, aggiungendosi ad essi impatti sociali decisamente complessi e a loro volta fonti di spese, costi e necessità di investimento. E ciò è tanto maggiore se vi si aggiungono danni fisici rilevanti, estesi ad una pluralità di soggetti.

¹ Per chi fosse interessato ad approfondire la questione, segnalo l'esistenza di alcuni studi specifici compiuti dall'American Psychological Association.

² L'ultima aggressione di Una bomber ha comportato la chiusura del supermercato per due giorni.

³ Il decremento delle vendite a seguito delle aggressioni di Unabomber è stato di circa il 20% per sei settimane, con un ritorno alla normalità in nove settimane.

3. AZIONI DI CONTRASTO.

Dopo aver sinteticamente illustrato il fenomeno del tampering nella sua valenza e portata, affrontiamo il problema, altrettanto complesso, delle possibilità di prevenzione e reazione.

Trattandosi, nel nostro caso, di azioni compiute a scopo di terrorismo, è palese che l'azione preventiva fondamentale sia quella svolta dai servizi di informazione e sicurezza, nell'ambito del costante sforzo volto alla tutela generale della nazione. Questa attività è, oltre che quella di maggior valenza complessiva, anche quella che ha nel tempo consentito di contenere il fenomeno in dimensioni estremamente contenute. Tornando al noto episodio dell'adulterazione dei pompelmi israeliani, notiamo come il fenomeno sia stato immediatamente circoscritto, al punto tale da impedirne la diffusione e la reiterazione. Si tratta, invero, di un caso estremo, sia per le modalità particolarmente pericolose con le quali venne condotto che per la decisione della risposta di Israele. Ma ben sappiamo che quel Paese ha capacità di risposta che gli altri paesi occidentali ben difficilmente possono mettere in atto, quantomeno con la medesima libertà di azione.

E' ovvio che l'attività di dissuasione e contrasto in esame, per sua natura, non possa essere oggetto di pubblico dibattito. Per riportare, quindi, l'analisi in campi per così dire misurabili, possiamo fare un raffronto con l'ondata di azioni terroristiche originate dall'Iraq in occasione del conflitto del 1991. In tale periodo, ristretto a soli 43 giorni, le varie compagini terroristiche sostenute dall'Iraq (peraltro tra le più pericolose del mondo arabo) pianificarono e tentarono circa 200 attentati: solo due furono portati a compimento¹.

Possiamo quindi affermare che il principale strumento di lotta al tampering a fini di terrorismo sia l'attività di intelligence e operativa dei servizi segreti.

Vi sono altre azioni di contrasto riferibili ad attività istituzionali, consistenti nel sistema di controlli esercitato sulle importazioni, sulla produzione e sulle reti distributive.

In Italia, pur non esistendo una rete di punti di controllo dedicata specificamente al rischio di tampering, queste verifiche sono piuttosto incisive. Esse partono dai controlli di frontiera esercitati dall'Amministrazione Doganale e dalla Guardia di Finanza e dai controlli alla produzione, per arrivare ai controlli sulla vendita esercitati da ASL, NAS e Polizia Annonaria. Un limite al meccanismo è posto dalla libera circolazione delle merci in ambito UE e da una serie di accordi commerciali con paesi non comunitari, alcuni dei quali forse non completamente affidabili. Vi sarà capitato di bere birra in un ristorante cinese: sull'etichetta vi è una dichiarazione in lingua italiana che afferma che essa è stata prodotta nella Repubblica Popolare Cinese in conformità delle leggi italiane in materia. Crederci è un puro atto di fede, che probabilmente esercitiamo inconsapevolmente anche nei confronti di buona parte del cibo che quella birra accompagna e che proviene dallo stesso Paese. Non è credibile che sia mai stata effettuata alcuna verifica presso la birreria Tsing Tao di Zhejiang, che peraltro è per la Cina un'industria di interesse nazionale.

Vi sono poi delle forme di controllo per così dire indiretto, consistenti nell'ormai complesso e diffuso sistema di normazione volontaria, norme UNI in testa. Lo scopo delle certificazioni non è certo quello di prevenire azioni di tampering, tuttavia è indubbio che un sistema di processi verificato e verificabile renda più sicura e controllabile l'attività delle aziende.

Un limite intrinseco di tale strumento è che l'unica vera garanzia che esso fornisce è che le cose siano sempre fatte nello stesso modo, il che include anche gli errori...

Alla categoria appartengono anche gli adempimenti di autocontrollo del sistema HACCP, che sarebbero un potente strumento di prevenzione se solo venissero effettivamente applicati con il dovuto rigore.

¹ Si tratta degli attentati alle rappresentanze diplomatiche USA di Djakarta e Manila. Nel primo caso l'ordigno venne disinnescato e nel secondo esplose anzitempo, uccidendo un terrorista e ferendone un altro.

Le aziende di dimensioni ragguardevoli, e fortunatamente anche –progressivamente- quelle di minore entità, si dotano quasi sempre di strutture, interne o esterne, di controllo di qualità. Questi sono, ai nostri fini, strumenti molto efficaci nel settore produttivo, mentre non sono presi in considerazione se non marginalmente, e per scopi di mera ottimizzazione, nella supply chain. Purtroppo, si tratta di strutture onerose per le aziende, che considerano oltretutto ancor più onerose le loro azioni.

In tale ottica, si devono ritenere più “sicure” le aziende che più rischiano in caso di eventi negativi, ossia le aziende di maggiori dimensioni o che producono articoli di elevata qualità e molto noti sul mercato. La necessità di tutela del marchio è quindi più sentita e giustifica anche sacrifici economici volti al mantenimento di elevati standard.

Ritroviamo qui una questione già posta: sono più sicuri o lo sono meno i sistemi complessi? Se da un lato complessità vuol dire processi più articolati e quindi maggiori occasioni di aggressione, dall'altro la complessità richiede adempimenti organizzativi che tendono ad essere più controllati e controllabili.

A valle dei processi produttivi, troviamo una realtà molto complessa e decisamente più a rischio: la supply chain o, più semplicemente, la catena logistica.

Troppo spesso, si tratta di una fase del ciclo nella quale la manipolazione dei prodotti alimentari è assai facile.

Dobbiamo qui distinguere, sostanzialmente, tre branche diverse: i deperibili e deperibilissimi, il secco e la logistica del freddo.

I prodotti deperibili e deperibilissimi sono per loro natura oggetto di una logistica molto rapida, generalmente in/out e senza giacenze a stock, per lo più svolta a temperature controllate e in un ristretto numero di fasi. Si tratta, in astratto, di un processo snello e che potrebbe essere quindi frettolosamente considerato più sicuro.

Tale valutazione viene meno se si considerano altri fattori:

- spesso per tali prodotti non vi è packaging o ve ne sono forme molto labili (vds. formaggi freschi incartati);
- molte referenze vengono trattate a collo o a peso medio, rendendo così vana ogni forma di controllo di congruenza quantitativa sufficientemente precisa da evidenziare manomissioni;
- si tratta quasi sempre di prodotti molto facilmente soggetti ad aggressione di agenti patogeni e spesso destinati a consumo senza cottura;
- la loro lavorazione all'origine viene sovente effettuata da soggetti non identificati né identificabili e con processi sommari (p. es. ortofrutta nella fase di raccolta);
- sono oggetto di distribuzione centralizzata, in piattaforme nelle quali è meno controllabile l'eventuale manipolazione anche su larga scala, o di consegne dirette ai punti vendita, rimanendo così alla mercè del trasportatore;
- presso i punti vendita, i prodotti sono spesso gestiti da merchandiser che –a spese dei fornitori- provvedono alla sistemazione a banco. Non sempre i merchandiser sono oggetto dei dovuti controlli, compresa l'identificazione;
- per loro natura, i prodotti sono esposti in vendita alla pubblica fede, il che assieme al packaging sommario rende molto facile la contaminazione e la remissione a banco.

Per il c.d. secco, o scatolame, valgono considerazioni del tutto diverse.

Da un lato si tratta di referenze per loro natura destinate alla conservazione a medio e lungo termine, e quindi protette da un packaging molto più consistente che spesso rende anche evidente la manomissione, pur non essendo tamper-evident. La conservazione e lo stoccaggio avvengono per lo più in pallet o comunque in colli la cui manomissione è visibile, e sono collocati in rack difficilmente raggiungibili perché distanti dal suolo, se si eccettua la fase di picking. Oltretutto, nei depositi spesso solo il sistema informatico sa esattamente dove si trovino le varie referenze.

Per contro, proprio i tempi lunghi di giacenza aumentano la possibilità di prelevare, manomettere ad arte e ricollocare le confezioni.

La fase di trasporto è generalmente oggetto di controlli, e quasi sempre le merci viaggiano su mezzi sigillati per problemi connessi ai furti ed alle contestazioni sulle quantità. Ma tutti gli operatori del settore hanno dolorosa esperienza della diffusa inosservanza delle procedure sigilli, e sono sempre più diffuse, specie per le piccole e medie superfici di vendita, le consegne multidrop (lo stesso mezzo consegna a più destinatari) che rendono più permeabile il sistema.

Anche presso i punti di vendita la giacenza si protrae per tempi anche lunghi, cosa che rappresenta il rischio di manomissioni anche elaborate.

Anche la velocità di rotazione delle referenze a scaffale può essere una criticità. Il recente caso di manomissione di un tubetto di bolle di sapone da parte dell'Unabomber del Nordest ne è la riprova. Le bolle di sapone non si vendono con la velocità dell'acqua minerale: non è così difficile acquistarne una confezione, manometterla e rimetterla poi al suo posto, magari non in prima fila. Accade, così, che il prodotto rimanga molto tempo nello scaffale prima della vendita, vanificando la possibilità di sfruttare i sistemi TVCC per scoprire l'autore del tampering, dato che le immagini video vengono conservate solo per breve tempo.

La logistica del freddo è a sua volta particolare. Le modalità di conservazione e di trasporto e la durezza dei materiali sono dei seri ostacoli alla manomissione, anche se il ricongelamento dei prodotti potrebbe aumentare la tossicità degli agenti patogeni resistenti alle basse temperature, che pure non sono molti. Si tratta, poi, di prodotti destinati alla cottura, il che complica ancor più la contaminazione biologica.

Il controllo delle superfici di vendita, infine, è un'altra area di grande criticità. I piccoli esercizi sono spesso caotici e sovraffollati, anche perché molti sorgono nei centri urbani ad elevata densità abitativa. Per contro, le grandi superfici pongono seri problemi di controllo. Per di più, la sorveglianza è generalmente rivolta alle referenze più soggette a furti, tra le quali non figurano quasi per nulla deperibili, deperibilissimi e gran parte dello scatolame.

Che il problema del controllo esista e sia serio è dimostrato dal fatto che, pur sorvegliate, le merci sono oggetto di taccheggio massiccio. In Europa, nella sola Grande Distribuzione, l'ammontare delle differenze inventariali nel 2001 è stato stimato in 30.311 miliardi di Euro, il 72,7% delle quali dovute a furti¹. Tanto basti.

Il rischio di tamper nelle produzioni interne, ossia nelle preparazioni alimentari confezionate presso i punti di vendita, è invece piuttosto basso. La lavorazione è compiuta da addetti esperti, e quindi ben conosciuti, la conservazione avviene in banchi non accessibili al pubblico e la vendita è effettuata in confezioni non alterabili. Sussistono margini di rischio per le preparazioni porzionate esposte al pubblico, che pure sono di difficile manomissione. Le aggressioni che si sono registrate sono imputabili a danneggiamento e non finalizzate a creare danni all'utente.

Tutti gli strumenti di controllo e le fasi dei processi condividono il vero fattore di rischio: l'uomo. Questo fattore aumenta esponenzialmente non già per scarsa attenzione alla sicurezza, ma per una "banale" questione di costi. Il personale addetto alla raccolta dei prodotti ortofrutticoli, al trasporto, al facchinaggio, al picking (soprattutto alla "ventilazione" dei deperibili, che vengono lavorati solo di notte) è costituito da forza lavoro di bassa specializzazione e ancor minore motivazione. In altissima percentuale, si tratta di cittadini extracomunitari ad elevato turnover ed il massiccio ricorso all'outsourcing sovente comporta l'impiego di cooperative che non vanno troppo per il sottile in materia di permessi di soggiorno e di controllo del personale. Le aziende spesso non esercitano controlli efficaci sugli accessi, preferendo tenere bassi i costi facendo finta di non sapere

¹ Fonte: Center for Retail Research, Nottingham, UK – The European Retail Theft Barometer.

e di non vedere. È qui che si annida il maggior margine di rischio. Chiunque abbia frequentato di Centri Distributivi ben conosce la situazione.

Ma questo stato di cose ben difficilmente è destinato a mutare nel breve periodo, almeno fino a quando non si chiuderanno le stalle dopo che i buoi saranno scappati: speriamo che non sia troppo tardi per qualche sfortunato consumatore.

4. UN ESEMPIO CONCRETO DI SISTEMA INTEGRATO DI PREVENZIONE DEL TAMPERING: LE PRDISPOSIZIONI ADOTTATE NEGLI USA.

Nell'ottica dei controlli istituzionali, merita particolare menzione il sistema di verifiche adottato recentemente dagli Stati Uniti¹, che entrerà a regime il 12 dicembre 2003².

Esso interessa tutta la produzione alimentare per uso umano ed animale, dalla produzione in avanti, ivi inclusi i prodotti dietetici, quelli per l'infanzia, le bevande, gli alcolici e gli additivi. Prevede un complesso sistema, basato su:

- un sistema di registrazione, gratuito, di tutti gli impianti di produzione, lavorazione, confezionamento, conservazione e distribuzione, sia negli USA che all'estero, con le sole eccezioni di fattorie, ristoranti, reparti di produzione alimentare del retail, organizzazioni non-profit e battelli da pesca;
- l'obbligo di notifica preventiva, da 5 giorni fino a 8 ore prima, di ogni importazione alimentare, con preciso dettaglio degli articoli e dichiarazione del luogo di introduzione nello stato;
- l'obbligo di determinare e mantenere la tracciabilità dei prodotti, completa di provenienza e destinazione, con la sola esclusione di fattorie e ristoranti;
- la possibilità di blocco alla frontiera non solo in caso di violazione degli obblighi sopra esposti ma anche a carico di soggetti che abbiano precedenti specifici in materia di reati connessi al settore alimentare;
- la marcatura dei cibi eventualmente respinti alla frontiera;
- la presunzione di adulterazione in caso di ulteriore tentativo di importazione di merci respinte;
- un sistema di rigide prescrizioni per le merci in transito negli USA (import for export), con la possibilità di respingere le merci in caso di legittimo sospetto che esse non abbiano tale destinazione.

In modo del tutto coordinato con la normativa contenuta nel Bioterrorism Act, il 21 marzo u.s. la FDA ha emanato quattro "guidance", ossia raccomandazioni e linee guida, due definitive e due provvisorie (vds. nota 2), rivolte alla prevenzione e sicurezza nei settori:

1. distribuzione alimentare e ristorazione;
2. industria e trasporto di cosmetici;
3. industria e trasporto alimentare;
4. importazione e filiere alimentari.

Lo scopo è quello di fornire alle aziende interessate uno strumento di controllo che possa minimizzare i rischi di tampering attraverso una rivisitazione delle procedure e dei controlli e

¹ Bioterrorism Act, cit.. Per maggiori notizie, consultare il sito <http://www.fda.gov/oc/bioterrorism/bioact.html>

² È interessante notare che si tratti, per il diritto americano, di "proposed regulation", ossia di norme che possono essere modificate in base ai commenti ed ai suggerimenti che chiunque può proporre nel termine di 60 giorni dalla data della loro pubblicazione sul Federal Register. L'entrata in vigore segue di sei mesi l'emanazione della legge (12 giugno - 12 dicembre).

l'adozione dei necessari correttivi. La loro struttura, quindi, segue l'analisi di processo delle attività del settore, focalizzando l'attenzione delle aziende sulle singole fasi.

Notiamo una raccomandazione che, in Italia, sarebbe assolutamente inutile e che sarà invece oggetto di grande attenzione negli USA: "Per avere successo, l'implementazione delle misure preventive di rinforzo richiede l'impegno della dirigenza e del personale ... La FDA raccomanda che sia il management che lo staff partecipino allo sviluppo ed alla revisione delle misure in questione".

Dichiaratamente, le guide non hanno pretesa di esaustività, essendo dirette ad una pluralità di soggetti di dimensioni e strutture molto diversi, e non intendono essere uno standard minimo, lasciando alle aziende l'adozione di misure efficienti ed efficaci sulla base dei propri specifici processi.

Si può però facilmente ipotizzare che i suggerimenti siano accolti con scrupolo ed attenzione e che il loro adempimento abbia riflessi importanti sia sotto il profilo della limitazione delle responsabilità civili e penali che sotto il profilo del rischio assicurativo. Queste considerazioni potrebbero rendere assai utile il loro "trapianto" anche in talune nostre realtà, decisamente carenti sotto il profilo normativo, ed è anche questo lo scopo per il quale ci diffondiamo nella loro disamina.

Le guide sono suddivise in cinque sezioni, a loro volta comprendenti diversi capitoli:

- management (preparazione alla possibilità degli eventi criminosi – supervisione – strategie di recall - investigazione su attività sospette – programma di valutazione);
- elemento umano: staff (sceening preassuntivo, assuntivo e post assunzione – assegnazione dei compiti quotidiani – identificazione – restrizione degli accessi – effetti personali – formazione in materia di procedure di sicurezza – comportamenti inusuali – salute degli operatori);
- elemento umano: pubblico (clienti – altri visitatori);
- strutture (sicurezza fisica – conservazione ed uso di sostanze pericolose, compresi i materiali di pulizia);
- attività (ricevimento dei prodotti – conservazione e stoccaggio – esposizione dei prodotti – sicurezza di acque e facilities [aria condizionata, refrigerazione, elettricità, combustibili, idranti, ecc.] – posta e pacchi – accesso ai sistemi informatici).

Le pubblicazioni sono completate da apparati puntuali di riferimento, come fonti informative complementari di settore, complete di indirizzi IP, recapiti di contatto per le emergenze e norme contenenti responsabilità penali.

A titolo di esempio, negli atti del convegno troverete la Guida per il retail e la ristorazione, edizione del 21 marzo 2003. Il restante materiale è reperibile sul sito

<http://www.fda.gov>

[U. S. Department of Health and Human Services](http://www.fda.gov)

U. S. Food and Drug Administration

Center for Food Safety and Applied Nutrition

Guida per il settore

Retail e imprese fornitrici di servizi di ristorazione: Guida alle misure preventive per la sicurezza degli alimenti

Versione in bozza

La presente bozza della guida rispecchia l'opinione attuale dell'Agenzia circa le misure che gli operatori del retail e di imprese fornitrici di servizi di ristorazione possono adottare per minimizzare il rischio che gli alimenti soggetti al loro controllo siano oggetto di manomissione o di altri atti dolosi, criminosi o terroristici. In quanto tale, non genera né conferisce alcun diritto a, o nei confronti di, terzi e non ha natura vincolante né per la FDA né per il pubblico.

Finalità e ambito di applicazione:

La presente bozza della guida è stata concepita come ausilio agli operatori del retail e delle aziende fornitrici di servizi di ristorazione (ad esempio, panetterie, bar, *bed & breakfast*, tavole calde, campeggi, istituti di assistenza giornaliera per adulti e bambini, cucine delle chiese, mense aziendali, enti di beneficenza, mini-market, fiere e mercati, banchi alimentari, drogherie, società di trasporti a lunga distanza di alimenti, servizi di consegna pasti a domicilio per invalidi o ammalati, chioschi itineranti, ristoranti e distributori automatici). Questo gruppo di operatori include società e negozi molto eterogenei e dalle più svariate dimensioni.

La presente bozza della guida identifica le azioni preventive che tali operatori possono adottare per minimizzare il rischio che gli alimenti sotto il loro controllo siano oggetto di manomissione o di altri atti dolosi, criminosi o terroristici. Gli operatori del retail e di società di servizi di ristorazione sono incoraggiati a riesaminare le procedure applicate e i controlli eseguiti attualmente alla luce del potenziale rischio di manomissioni o di altri atti dolosi, criminosi o terroristici, e di apportarvi quindi le modifiche appropriate.

La presente guida in bozza è stata realizzata con l'obiettivo di focalizzare l'attenzione dell'operatore, in sequenza, su ogni singolo segmento del sistema di distribuzione degli alimenti di

loro competenza, al fine di minimizzare il rischio di manomissioni o di altri atti dolosi, criminosi o terroristici compiuti ai danni di ciascun segmento. Affinché le misure preventive di sicurezza abbiano successo, la loro implementazione richiede il coinvolgimento sia del management sia del resto del personale. Di conseguenza, la FDA raccomanda che sia il management sia il resto del personale partecipino allo sviluppo e alla revisione di tali misure.

Limitazioni:

Non tutte le linee-guida contenute nel presente documento risultano adeguate ad ogni singola rivendita di prodotti alimentari o società fornitrice di servizi di ristorazione, e questo vale in particolare per le unità di piccole dimensioni. La FDA consiglia agli operatori di prendere visione delle sezioni della presente guida che fanno riferimento ad un componente della propria attività specifica, e quindi di valutare quali sono le misure preventive più adeguate al loro contesto specifico. Per molte delle misure preventive contenute nel presente documento vengono forniti esempi di approccio alla problematica. Tali esempi non devono essere considerati degli standard minimi, così come l'insieme degli esempi forniti non è da ritenersi un elenco completo di tutti i possibili approcci potenziali finalizzati al conseguimento dell'obiettivo della misura preventiva in oggetto. La FDA raccomanda agli operatori di considerare l'obiettivo della misura preventiva, di valutare se tale obiettivo è pertinente alla loro attività e, in caso lo sia, di elaborare un approccio che sia al tempo stesso efficiente ed efficace ai fini del raggiungimento dell'obiettivo nel contesto dell'attività da loro svolta.

Struttura del testo:

La presente guida è suddivisa in cinque sezioni relative ai singoli componenti dell'attività del retail e delle imprese che forniscono servizi di ristorazione: management; elemento umano -- il personale; elemento umano – il pubblico; struttura, e attività.

Guide correlate:

La FDA ha pubblicato altre due guide sulla sicurezza degli alimenti dal titolo: "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance" ("Imprese di produzione, lavorazione e trasporto di generi alimentari: Guida alle misure preventive per la sicurezza degli alimenti") e "Importers and Filers: Food Security Preventive Measures Guidance" ("Importatori e filiere: Guida alle misure preventive per la sicurezza degli alimenti"), così da coprire

l'intero processo di produzione degli alimenti, dall'agricoltore al consumatore. Entrambi i documenti sono disponibili sul sito: http://www.access.gpo.gov/su_docs/aces/aces140.html.

Risorse supplementari:*

Il processo denominato Operational Risk Management – ORM (Gestione del Rischio Operativo) può risultare utile per assegnare una priorità alle misure preventive che verosimilmente potranno avere un maggiore impatto sulla riduzione del rischio di manomissione o di atti dolosi, criminosi o terroristici perpetrati a danno degli alimenti. Maggiori informazioni sull'ORM sono disponibili nel Federal Aviation Administration (FAA) System Safety Handbook, pubblicato dal U.S. Department of Transportation, FAA, il 30 dicembre 2000, al Capitolo 15: Operational Risk Management. Il manuale è disponibile sul sito: http://www.asy.faa.gov/Risk/SSHandbook/Chap15_1200.PDF

Il U.S. Department of Transportation, Research and Special Programs Administration ha emanato una comunicazione con valore consultivo sull'adozione di misure volontarie per aumentare la sicurezza delle spedizioni di materiali pericolosi. E' disponibile sul sito: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-3636-filed.pdf. Il comunicato fornisce delle linee-guida agli spedizionieri marittimi e ai vettori sulle questioni di sicurezza relative al personale, alle strutture e al trasporto.

Il U.S. Postal Service ha redatto una guida per l'identificazione e lo smistamento di posta sospetta. La guida è disponibile sul sito: <http://www.usps.com/news/2001/press/mailsecurity/postcard.htm>.

In base al Federal Anti-Tampering Act (18 USC 1365), costituisce reato federale manomettere o contaminare un prodotto di consumo, o tentare di, minacciare di, o associarsi per manomettere o contaminare un prodotto di consumo, oppure rilasciare dichiarazioni false in cui si annuncia di aver manomesso o contaminato un prodotto di consumo. In caso di verdetto di colpevolezza si prevedono pene fino all'ergastolo e multe fino a un massimo di \$100.000. Il testo della legge è disponibile sul sito: <http://www.fda.gov/opacom/laws/fedatact.htm>.

Il National Infrastructure Protection Center (NIPC) funge da centro del governo federale dedicato alla valutazione, segnalazione, investigazione e risposta a minacce o attacchi rivolti contro infrastrutture statunitensi di importanza critica. Il NIPC ha identificato il sistema di distribuzione degli alimenti come una delle otto infrastrutture di importanza critica e costituito una partnership pubblico-privata con il settore alimentare concretizzata nel Food Industry Information & Analysis Center – Centro di Informazioni e Analisi per l'Industria Alimentare (Food Industry ISAC). Il NIPC fornisce al Food Industry ISAC l'accesso a risorse, informazioni e analisi che consentono al settore alimentare di segnalare, identificare e ridurre i propri punti vulnerabili agli attacchi intenzionali e a riprendersi da tali attacchi nel più breve tempo possibile. In particolare, il NIPC identifica le minacce credibili ed elabora specifici messaggi di allerta per il settore alimentare. Ulteriori informazioni sono disponibili sui siti <http://www.nipc.gov/> e <http://www.foodisac.org/>.

Infine, la FDA incoraggia le associazioni di categoria a valutare le misure preventive contenute nella presente guida, ad adeguarle ai propri prodotti e alle attività specifiche svolte, e ad integrare la presente guida con misure preventive supplementari ove del caso. La FDA è aperta al dialogo con le associazioni di categoria competenti circa i contenuti delle linee-guida settoriali.

Attività di retail alimentare e delle imprese fornitrici di servizi di ristorazione:

Management

La FDA raccomanda agli operatori del retail e delle imprese di ristorazione di prendere in considerazione la necessità di:

- prepararsi all'eventualità di manomissioni o di altri atti dolosi, criminosi o terroristici
 - affidare la responsabilità della sicurezza a uno o più individui competenti
 - effettuare una valutazione iniziale delle procedure e delle operazioni di sicurezza relative agli alimentari, che si consiglia di mantenere riservate
 - disporre di una strategia per la gestione delle crisi che consenta di prepararsi e di reagire alle manomissioni e agli altri atti dolosi, criminosi o terroristici – sia minacce sia eventi reali –, e che includa l'individuazione, l'isolamento e la collocazione in un luogo sicuro dei prodotti interessati
 - pianificare un'eventuale evacuazione di emergenza, con misure che impediscano violazioni della sicurezza durante l'evacuazione
 - familiarizzare con il sistema di risposta alle emergenze esistente nella comunità
 - sensibilizzare il management sulla necessità di designare persone di riferimento che possano fornire informazioni 24 ore su 24 a polizia/vigili del fuoco/protezione civile/autorità sanitarie/agenzie per la sicurezza nazionale locali, statali e federali
 - comunicare al personale quali sono i membri del management cui vanno riportati gli eventuali potenziali problemi di sicurezza (persone di riferimento per coprire le 24 ore)

- promuovere una maggiore consapevolezza delle problematiche legate alla sicurezza degli alimenti per incoraggiare tutto il personale a prestare attenzione a qualsiasi indizio di manomissione o azione dolosa, criminosa o terroristica o ad aree che potrebbero essere vulnerabili ad azioni di questo tipo, e a segnalare qualunque scoperta ai membri del management designati (ad esempio, fornendo un addestramento specifico, istituendo un sistema di ricompense, inserendo la sicurezza negli standard di valutazione della performance)
- disporre di un sistema interno di comunicazione per informare e aggiornare il personale su questioni rilevanti per la sicurezza
- disporre di una strategia di comunicazione verso il pubblico (ad esempio, individuando un portavoce per i media, preparando comunicati stampa generici e informazioni di base, e coordinando i comunicati stampa con le autorità competenti)

• Supervisione

- fornire un livello adeguato di supervisione su tutto il personale, inclusi gli addetti alle pulizie e alla manutenzione, il personale a contratto, il personale di supporto addetto all'informatica e all'inserimento dati e, in particolare, al personale nuovo (ad esempio, supervisore in servizio, visite periodiche non programmate del supervisore, visite giornaliere del supervisore, due persone in servizio contemporaneamente, telecamere sorvegliate, visione a posteriori dei nastri registrati, finestre con vetri uni- e bidirezionali, feedback del cliente al supervisore su comportamenti insoliti o sospetti da parte del personale)
- eseguire controlli di routine della sicurezza della struttura, inclusi i sistemi di erogazione di energia, acqua, condizionamento, ecc. e i sistemi informatici di importanza critica (con una frequenza commisurata al tipo di attività svolto), per rilevare gli eventuali segni di manomissione o di atti dolosi, criminosi o terroristici, o le aree che potrebbero essere vulnerabili ad atti di questo genere

• Indagini sulle attività sospette

- indagare su minacce di manomissione o di altri atti dolosi, criminosi o terroristici, o su informazioni relative a segni di manomissione o altri atti dolosi, criminosi o terroristici
- informare le autorità di polizia e sanitarie competenti di qualunque minaccia o sospetto di manomissione o atti dolosi, criminosi o terroristici

• Programma di valutazione

- valutare le lezioni apprese da precedenti manomissioni o altri atti dolosi, criminosi o terroristici compiuti o minacciati

- rivedere e verificare, con cadenza almeno annuale, l'efficacia del programma di gestione della sicurezza (ad esempio, utilizzando personale competente interno o esterno per effettuare esercitazioni con simulazione di manomissioni o di altri atti dolosi, criminosi o terroristici e per mettere alla prova i sistemi di sicurezza della rete informatica), modificare il programma in base ai risultati ottenuti (servendosi di un esperto di sicurezza esterno o interno, ove possibile) e mantenere riservate queste informazioni
- eseguire a caso ispezioni finalizzate a garantire la sicurezza degli alimenti in tutte le aree della struttura (incluse le aree di entrata merci e di magazzino, ove possibile) servendosi di personale competente interno o esterno, e mantenere riservate queste informazioni
- quando possibile, verificare che i fornitori di servizi di sicurezza stiano lavorando in modo appropriato

Elemento umano – il personale

In base al diritto federale, si richiede agli operatori del retail e delle imprese di servizi di ristorazione di verificare l'idoneità all'impiego di tutti i nuovi assunti, in conformità con le disposizioni dell'Immigration and Nationality Act, compilando il modulo INS Employment Eligibility Verification Form (INS Form I-9). La compilazione del Form I-9 per i nuovi assunti è richiesta in base alla legge 8 USC 1324a, e le disposizioni anti-discriminazione relative al processo di verifica sono espone al par. 1324b.

La FDA raccomanda agli operatori del retail e delle imprese di ristorazione di prendere in considerazione la necessità di:

- eseguire uno screening (prima, durante e dopo l'assunzione)
 - esaminare il *background* di tutto il personale (inclusi i lavoratori stagionali, temporanei, a contratto e i volontari, sia che siano stati assunti direttamente che attraverso una società di ricerca del personale) per verificarne l'adeguatezza alle diverse posizioni, considerare la possibilità di accesso dei candidati ad aree riservate della struttura e il grado di supervisione cui saranno soggetti, oltre ad altri fattori di rilevanza (ad esempio, ottenendo e verificando referenze, indirizzi e numeri di telefono, aderendo ad uno dei programmi pilota gestiti dall'Immigration and Naturalization Service e dalla Social Security Administration. [Questi programmi forniscono la conferma elettronica dell'idoneità all'impiego dei nuovi assunti. Per ulteriori informazioni telefonare al numero verde dell'INS SAVE Program: 1-888-464-4218, inviare un fax di richiesta di informazioni al numero (202) 514-9981, o scrivere a: US/INS, SAVE Program, 425 I Street, NW, ULLICO-4th Floor, Washington, DC 20536. Questi programmi pilota potrebbero non essere disponibili in tutti gli stati], effettuando un controllo della fedina penale dei candidati attraverso

la polizia locale o un'agenzia competente [consultare prima le leggi statali o locali che possono eventualmente applicarsi all'esecuzione di controlli di questo genere])

- Nota: le procedure di screening dovrebbero essere applicate in modo uguale a tutto il personale, indipendentemente dalla razza, dalla nazione di provenienza, dalla religione, e dal fatto che il singolo lavoratore abbia la cittadinanza del Paese o ancora lo status di immigrato

- Assegnazione delle mansioni giornaliere

- sapere chi si trova e chi dovrebbe trovarsi all'interno della struttura, e quale dovrebbe essere la postazione di ognuno, per ogni turno di lavoro
- tenere aggiornate le informazioni

- Identificazione

- istituire un sistema di identificazione e riconoscimento sicuri (ad esempio, fornendo uniformi, targhette con il nome della persona o *badge* d'identificazione con foto e numero di controllo personale, di colore diverso a seconda dell'area in cui è autorizzato l'accesso), ove del caso
- ritirare le uniformi, la targhetta con nome o il *badge* di identificazione quando cessa il rapporto di lavoro fra il dipendente e la società

- Aree ad accesso limitato

- identificare il personale che deve avere accesso illimitato a tutte le aree della struttura
- rivedere periodicamente i livelli di accesso di tutti i dipendenti
- limitare l'accesso del personale alle aree non pubbliche, così che i dipendenti entrino soltanto nelle aree necessarie allo svolgimento delle rispettive mansioni e solamente durante ore di lavoro appropriate (ad esempio, utilizzando schede o dispositivi di apertura/chiusura con chiave o con codice per gli ingressi nelle aree riservate, uniformi di colore diverso a seconda delle aree cui si può accedere [consultare le eventuali disposizioni contro gli incendi o relative alla sicurezza sul lavoro federali, statali o locali prima di effettuare qualunque modifica])
- cambiare le combinazioni, i codici e le chiavi dei dispositivi di chiusura e/o ritirare la scheda in possesso del dipendente quando cessa il rapporto di lavoro fra quest'ultimo e la società, e inoltre in tutti i casi in cui ciò si riveli necessario per garantire la sicurezza

• Oggetti personali

- limitare i tipi di oggetti personali che è permesso introdurre nelle aree della struttura non aperte al pubblico
- autorizzare l'introduzione nelle aree della struttura chiuse al pubblico solo delle medicine per uso personale strettamente necessarie per tutelare la salute del personale (oltre a quelle immagazzinate o esposte a fini di vendita) e accertare che tali medicine per uso personale siano adeguatamente etichettate e poste lontano dai generi alimentari conservati all'interno della struttura e dalle aree adibite alla preparazione dei cibi
- impedire al personale di introdurre oggetti personali (ad esempio, contenitori per il pranzo, borse, ecc.) nelle aree non aperte al pubblico adibite alla preparazione o allo stoccaggio degli alimenti
- effettuare regolarmente ispezioni del contenuto degli armadietti dei dipendenti (ad esempio, installando armadietti con sportello in rete metallica, richiedendo che vengano usati lucchetti forniti dall'azienda), di borse, pacchetti e veicoli quando questi si trovino nella proprietà dell'azienda (consultare prima le eventuali leggi federali, statali o locali relative a tali ispezioni)

Formazione sulle procedure per garantire la sicurezza degli alimenti

- introdurre strumenti che diffondano la consapevolezza dell'importanza della sicurezza degli alimenti, incluse informazioni su come impedire, rilevare e reagire alle manomissioni o ad altri atti dolosi, criminosi o terroristici o a minacce di tali atti, nei programmi di formazione per il personale, compresi i lavoratori stagionali, temporanei e a contratto e i volontari
- ricordare periodicamente l'importanza delle procedure di sicurezza (ad esempio, organizzando riunioni, distribuendo opuscoli, inserendo comunicazioni al riguardo nella busta paga)
- incoraggiare il supporto da parte del personale (ad esempio, coinvolgendo il personale nella pianificazione della sicurezza degli alimenti e nel programma di diffusione della consapevolezza del problema della sicurezza alimentare, dimostrando al personale l'importanza delle procedure di sicurezza)

• Comportamenti insoliti

- individuare e sorvegliare eventuali comportamenti insoliti o sospetti da parte del personale (ad esempio, dipendenti che, senza uno scopo identificabile, si trattengono insolitamente a lungo dopo la fine del proprio turno di lavoro, arrivano insolitamente presto, accedono a file/documenti/informazioni/aree della struttura al di fuori delle aree di loro competenza; portano documenti fuori dalla struttura; fanno domande su argomenti riservati; portano macchine fotografiche sul posto di lavoro)

- Stato di salute del personale

- prestare attenzione alle condizioni di salute atipiche del personale segnalate volontariamente dai dipendenti interessati e alle assenze che potrebbero essere un primo indicatore di manomissione o del compimento di altre azioni di natura dolosa, criminosa o terroristica (ad esempio, un numero insolitamente elevato di dipendenti che lavorano nella stessa area della struttura che segnalano sintomi simili in un breve arco di tempo), e segnalare tali condizioni alle autorità sanitarie locali

Elemento umano – il pubblico

La FDA raccomanda agli operatori del retail e delle imprese di ristorazione di prendere in considerazione la necessità di:

- Clienti

- impedire l'accesso alle aree adibite alla preparazione e allo stoccaggio degli alimenti e al lavaggio delle stoviglie e collocate nella parte non aperta al pubblico della struttura, incluse le rampe di carico
- tenere sotto controllo le aree pubbliche, inclusi gli ingressi ai bagni pubblici (ad esempio, utilizzando guardie di sicurezza, telecamere sorvegliate, finestre con vetri uni- e bidirezionali, collocando le postazioni dei dipendenti in modo tale da consentire una visibilità ottimale) per individuare le attività insolite o sospette (ad esempio, un cliente che mette sullo scaffale un prodotto che ha introdotto nel negozio da fuori, che trascorre un periodo di tempo insolitamente lungo in una determinata area nel negozio)
- tenere sotto controllo il servizio o l'esposizione degli alimenti nelle aree self-service (ad esempio, i banchi delle insalate, i condimenti, i contenitori aperti contenenti prodotti sfusi, le aree di esposizione dei prodotti, gli scatoloni di brioches/merendine)

- Altri visitatori (ad esempio, fornitori, rappresentanti, autisti addetti alle consegne, corrieri, rappresentanti dell'ufficio disinfestazione, revisori esterni, autorità, giornalisti, visite guidate)

- limitare l'ingresso nelle aree della struttura non aperte al pubblico (ad esempio, controllando i visitatori in entrata e in uscita dalle aree non aperte al pubblico, richiedendo un documento di identità, rilasciando badge per i visitatori che devono essere ritirati quando il visitatore lascia la struttura, accompagnando i visitatori)

- accertare che esista un valido motivo per tutte le visite alle aree della struttura non aperte al pubblico prima di consentire l'accesso alle stesse – fare attenzione ai visitatori non previsti
- verificare l'identità dei visitatori sconosciuti che accedono alle aree della struttura chiuse al pubblico
- ispezionare, nella misura in cui ciò sia possibile, i pacchi e le valigette che entrano ed escono dalle aree della struttura non aperte al pubblico per verificare che non contengano oggetti sospetti, impropri o insoliti

Struttura

La FDA raccomanda agli operatori del retail e delle imprese di ristorazione di prendere in considerazione la necessità di:

• Sicurezza fisica

- proteggere il perimetro dell'area non aperta al pubblico con recinzioni o altri deterrenti, ove del caso
- bloccare, per quanto possibile, le porte (incluse le porte di carico merci, quando non utilizzate e non controllate, e le uscite d'emergenza), le finestre, le aperture, i lucernari sul tetto, le bocche di sfiato, i sistemi di ventilazione, i ripostigli, le stanze di stoccaggio e di produzione del ghiaccio, i solai, i rimorchi e i serbatoi per i liquidi, i solidi e i gas compressi (ad esempio, utilizzando lucchetti e serrature, sigilli, allarmi, sensori anti-intrusione, guardie, telecamere sorvegliate [consultare le eventuali disposizioni contro gli incendi o relative alla sicurezza sul lavoro federali, statali o locali prima di effettuare qualunque modifica])
- utilizzare, nei limiti del possibile, porte esterne di metallo o rivestite in metallo quando la struttura non è operativa, eccetto nei casi in cui la visibilità da vie di grande passaggio è intenzionalmente utilizzata come deterrente (consultare le eventuali disposizioni contro gli incendi o relative alla sicurezza sul lavoro federali, statali o locali prima di effettuare qualunque modifica)
- ridurre al minimo il numero di ingressi alle aree chiuse al pubblico (consultare le eventuali disposizioni contro gli incendi o relative alla sicurezza sul lavoro federali, statali o locali prima di effettuare qualunque modifica)
- tenere un resoconto di tutte le chiavi utilizzate per l'accesso ai vari locali della struttura (ad esempio, affidando ad alcuni dipendenti la responsabilità del rilascio, del monitoraggio e del ritiro delle chiavi)
- monitorare la sicurezza dei locali utilizzando metodi appropriati (ad esempio, servendosi di pattuglie di sorveglianza [in uniforme e/o in abiti civili], di video-sorveglianza con monitoraggio)

- ridurre al minimo, nei limiti del possibile, i luoghi all'interno delle aree pubbliche in cui un intruso potrebbe rimanere, inosservato, anche dopo il termine dell'orario di lavoro
 - ridurre al minimo, nei limiti del possibile, i luoghi all'interno delle aree chiuse al pubblico che potrebbero essere utilizzati per nascondere temporaneamente sostanze da utilizzare per contaminazioni intenzionali (ad esempio, limitando il numero di recessi, controsoffitti, ecc.)
 - fornire un'illuminazione adeguata all'interno e all'esterno, incluso un sistema di illuminazione di emergenza, ove opportuno, per facilitare l'individuazione di attività sospette o insolite
 - implementare un sistema per il controllo dei veicoli autorizzati a parcheggiare nelle aree di parcheggio chiuse al pubblico (ad esempio, utilizzando appositi talloncini o decalcomanie, schede magnetiche, dispositivi di apertura con chiave o con codice, rilasciando *pass* per aree e orari specifici per i veicoli dei visitatori)
 - ove possibile, separare le aree di parcheggio per i clienti, i dipendenti e i visitatori dagli ingressi alle aree chiuse al pubblico
- Stoccaggio e utilizzo di sostanze chimiche velenose e tossiche (ad esempio, detergenti e disinfettanti, pesticidi) nelle aree non pubbliche
- limitare la presenza all'interno della struttura di sostanze chimiche tossiche e velenose a quelle effettivamente necessarie per la pulizia e la manutenzione della struttura e a quelle stoccate o esposte ai fini della vendita al dettaglio
 - porre le sostanze chimiche velenose e tossiche il più lontano possibile dalle aree in cui vengono manipolati e immagazzinati gli alimenti
 - limitare l'accesso alle aree di stoccaggio di sostanze chimiche velenose o tossiche non destinate alla vendita al dettaglio e chiuderle (ad esempio, utilizzando dispositivi di apertura/chiusura con chiave o codice, schede, sigilli, allarmi, sensori anti-intrusione, guardie, telecamere sorvegliate [consultare le eventuali disposizioni contro gli incendi federali, statali o locali prima di effettuare qualunque modifica])
 - accertare che le sostanze chimiche velenose e tossiche siano correttamente etichettate
 - utilizzare i pesticidi conformemente al Federal Insecticide, Fungicide, and Rodenticide Act (ad esempio, tenendo l'esca per i roditori utilizzata in appositi contenitori coperti e anti-manomissione)
 - essere a conoscenza dell'eventuale presenza di sostanze chimiche velenose e tossiche all'interno della struttura e mantenersi aggiornati circa la loro posizione e gli eventuali spostamenti
 - indagare sulle eventuali quantità mancanti dallo stock o su altre irregolarità al di fuori dei normali limiti di tolleranza, e segnalare alle forze di polizia e all'autorità sanitaria locali gli eventuali problemi irrisolti, ove opportuno

Attività

La FDA raccomanda agli operatori del retail e delle imprese di ristorazione di prendere in considerazione la necessità di:

- Prodotti in entrata

- utilizzare (ove possibile) soltanto fonti note e in possesso delle licenze o delle autorizzazioni appropriate per l'approvvigionamento di tutti i prodotti in entrata
- informare i fornitori, i distributori e i trasportatori dell'esistenza delle guide sulla sicurezza alimentare pubblicate dalla FDA e intitolate "Food producers, processors, and transporters: Food security preventive measures guidance" ("Imprese di produzione, lavorazione e trasporto di generi alimentari: Guida alle misure preventive per la sicurezza degli alimenti") e "Importers and filers: Food security preventive measures guidance", ("Importatori e filiere: Guida alle misure preventive per la sicurezza degli alimenti"), disponibili sul sito: http://www.access.gpo.gov/su_docs/aces/aces140.html.
- adottare misure che garantiscano che i veicoli utilizzati per le consegne siano adeguatamente sicuri
- richiedere che i trasportatori dispongano di strumenti che permettano di verificare in qualsiasi momento dove si trova il carico, ove possibile
- definire un piano di schedulazione delle consegne, non accettare le consegne o gli autisti non programmati e ingiustificati e indagare sulle eventuali consegne in ritardo o mancanti
- effettuare la supervisione delle operazioni di scarico della merce, anche in caso di consegne fuori orario
- confrontare e riconciliare i prodotti e gli importi ricevuti con i prodotti e gli importi ordinati e con i prodotti e gli importi elencati sulla fattura e sui documenti di trasporto, tenendo conto di eventuali campionature effettuate prima del ricevimento del carico considerato
- indagare sull'origine di documenti di trasporto che riportano modifiche sospette
- ispezionare, ove opportuno, i prodotti in arrivo e i resi di prodotto per individuare l'eventuale presenza di segni di manomissione, contaminazione o danni (ad esempio, presenza di odori insoliti, di tracce anormali di polveri, liquidi o macchie, di segni che indicano chiaramente che l'imballo è stato aperto e risigillato o che l'imballo speciale anti-manomissione è stato danneggiato) o di "contraffazione" (ad esempio, specifiche o codici lotto del prodotto, etichette, identità del prodotto impropri o non corrispondenti, assenza dello speciale imballo anti-manomissione quando invece l'etichetta ne segnala la presenza),
- respingere i generi alimentari sospetti

- segnalare alle forze di polizia e alle autorità sanitarie competenti l'eventuale presenza di prove di manomissione, di "contraffazione" o di altri atti dolosi, criminosi o terroristici

- Magazzinaggio

- disporre di un sistema per il ricevimento, il magazzinaggio e la movimentazione dei prodotti deteriorati, danneggiati e resi e dei prodotti lasciati dai clienti alle casse, che riduca al minimo il potenziale di compromissione degli stessi (ad esempio, farsi motivare il reso e richiedere una prova dell'identità della persona che effettua il reso del prodotto, esaminare gli articoli resi o abbandonati al fine di individuare eventuali segni di manomissione, non rivendere i prodotti resi o abbandonati)
- tenere traccia dei prodotti in entrata, dei materiali utilizzati, dei prodotti recuperati e dei prodotti resi
- indagare sulle quantità mancanti o in eccesso di merce a magazzino o su altre irregolarità al di fuori dei normali limiti di tolleranza e segnalare gli eventuali problemi irrisolti alle forze di polizia e alle autorità sanitarie competenti, ove opportuno
- ridurre al minimo, ove possibile, il riutilizzo di contenitori, imballi per trasporto, cartoni, ecc.

- Esposizione di alimenti per vendita al dettaglio e finalizzata al servizio di ristorazione

- esporre le sostanze chimiche velenose e tossiche destinate alla vendita al dettaglio in un luogo che consenta di monitorarle con facilità (ad esempio, in luoghi visibili al personale dalla postazione di lavoro, da finestre e attraverso telecamere)
- effettuare, nei limiti del possibile, controlli periodici dei prodotti esposti per la vendita al dettaglio al fine di individuare la presenza di eventuali segni di manomissione o di altri atti dolosi, criminosi o terroristici (ad esempio, controllando: che il prodotto non si presenti in cattive condizioni [ad es. con confezione che perde, macchiata, danneggiata, con etichette mancanti o sbagliate]; che vi sia una corretta rotazione di magazzino; che le confezioni non siano state risigillate; in che condizioni sono le speciali confezioni anti-manomissione; che non vi siano confezioni vuote di prodotti alimentari o altri detriti e avanzi sugli scaffali)
- tenere sotto controllo le aree self-service (ad esempio, i banchi delle insalate, i condimenti, i contenitori aperti contenenti prodotti sfusi, le aree di esposizione dei prodotti, gli scatoloni di brioches/merendine) al fine di individuare eventuali segni di manomissione o di altri atti dolosi, criminosi o terroristici

- Sicurezza dell'acqua e dei pubblici servizi erogati

- limitare, nei limiti del possibile, l'accesso ai quadri di controllo/comandi di ventilazione, acqua, elettricità e refrigerazione

- bloccare l'accesso a pozzi idrici non municipali, idranti, impianti di magazzinaggio e movimentazione
- accertare che i camion-cisterna e gli impianti idrici siano dotati di dispositivi anti-riflusso
- trattare con cloro gli impianti idrici non municipali e tenere sotto controllo gli impianti di clorazione e i livelli di cloro
- testare la potabilità delle fonti non municipali, sia regolarmente sia a campione, e fare attenzione ai cambiamenti nel profilo dei risultati
- prestare attenzione, ove possibile, agli annunci da parte dei media che segnalano eventuali problemi delle società pubbliche di erogazione dell'acqua
- individuare fonti alternative di acqua potabile da utilizzare nelle situazioni di emergenza in cui i normali impianti di erogazione idrica risultino compromessi (ad esempio, acqua in bottiglia, cisterne provenienti da una fonte approvata, trattamento in loco o mantenimento di scorte di acqua in loco)

• Posta/pacchi

- implementare procedure che garantiscano la sicurezza della posta e dei pacchi in arrivo

• Accesso ai sistemi informatici

- limitare l'accesso ai sistemi informatici d'importanza critica a coloro in possesso di autorizzazioni appropriate (ad esempio, utilizzando password, firewall)
- inibire l'accesso al sistema informatico alle persone che non fanno più parte del personale della società
- installare un sistema che consenta la tracciabilità delle operazioni effettuate nel sistema informatico
- verificare l'adeguatezza dei sistemi anti-virus e delle procedure di back-up dei sistemi informatici d'importanza critica
- convalidare il sistema di sicurezza del sistema informatico

Da contattare in caso di emergenza:

U.S. Food and Drug Administration
5600 Fishers Lane

Rockville, MD 20857
301-443-1240

Nel caso in cui un operatore del retail alimentare o di una società erogatrice di servizi di ristorazione sospetti che qualcuno dei suoi prodotti regolamentati dalle norme della FDA sia stato oggetto di manomissione, “contraffazione”, o di altri atti dolosi, criminosi o terroristici, la FDA raccomanda che l’operatore effettui una segnalazione telefonando al numero di emergenza della FDA 301-443-1240, attivo 24 ore su 24, oppure all’ufficio della FDA del suo distretto. La FDA raccomanda che venga effettuata una segnalazione anche alle autorità sanitarie e alle forze di polizia locali.

I numeri di telefono degli uffici distrettuali della FDA sono disponibili sul sito:
http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html.

*I riferimenti a questi documenti hanno fini esclusivamente informativi. Questi documenti non sono inclusi per riferimento nella presente guida e non devono perciò essere considerati parte delle linee-guida fornite dalla FDA.
